بسم الله الرحمن الرحيم



جامعة مؤتة

عمادة الدراسات العليا

أثر التهديدات الأمنية في أمن المعلومات في ضوء تطبيق الحكومة الإلكترونية دراسة ميدانية

آمنه ماجد الربيحات

رسالة

مقدمة إلى

عمادة الدراسات العليا

استكمالاً لمتطلبات الحصول على

درجة الماجستير في الإدارة العامة قسم الإدارة العامة

جامعة مؤتة 2004

جامعة مؤته

عمادة الدراسات العليا

إجازة رسائل جامعية

تقرر إجازة الرسالة المقدمة من الطالبة آمنة ماجد الربيحات والموسومة بـ:

"اثر التهديدات الأمنية في أمن المعلومات في ضوء تطبيق الحكومة الالكترونية في عدد من الوزارات وأمانة عمان الكبرى".

استكمالا لمتطلبات الحصول على درجة الماجستير في الإدارة العامة .

القسم : الادارة العامة

الاسم	التوقيع	التاريخ	
د. صلاح الدين الهيتي		٢٠٠٤/١/٧	مشرفا
أ.د حلمي يوسف شحادة		٢٠٠٤/١/٧	عضوا
د. زياد يوسف المعشر		٢٠٠٤/١/٧	عضوا
د. موفق فتحي حسن		٢٠٠٤/١/٧	عضوا

عميد الدراسات العليا

د.ذياب البداينــة



الإهداء

إلى من امرني الله سبحانه وتعالى بالبر والإحسان إليهما، فقال في محكم تنزيلـــه "وقضى ربك ألا تعبدوا إلا إياه وبالوالدين إحساناً" إلى والدي العزيزين.

والى من اسبغ الله عليه النعمة والفضل، فجاد بهما علي، إلى من اشدد به أزري، وأجلي به همي وحزني، إلى الحبيب، والرفيق، والصديق، والأخ، الذي غمرني بجميله إلى أخي"حسن".

إلى الغاليات والحبيبات أخواتي، أم يزيد، وأم المعتــز بـــالله، وإيمـــان، والـــى أزواجهن وأولادهن.

إلى اخوتي: أبو مجد، وأبو زيد، وأبو ماجد، ومحمد، وزوجاتهم وأولادهم.

أمنه ماجد عبداللطيف الربيحات

شكر وتقدير

الحمد والشكر لله الذي وهبني الصبر والعزم على متابعة تعليمي، ويسر لي السبل لاتمام رسالتي هذه التي جاءت بإشراف أستاذي الفاضل وأخي في الله المربي الأستاذ الدكتور صلاح الدين الهيتي الذي احسن الله خلقه وخلقه وتعلمت منه ركيزة ديني، وهي المعاملة الحسنة، فله مني خالص الشكر والتقدير على جهوده الطيبة التي بذلها خلال مراحل دراستي للماجستير، واسال الله ان يعلي قدره ومنزلته في الدنيا والآخرة.

كما أقدم الشكر والامتنان إلى الدكتور الفاضل نضال الحوامده الذي لم يتأخر عن تقديم العون والمساعدة، وإبداء الملاحظات التي أثرت رسالتي، والشكر الموصول أيضاً لأساتذتي أعضاء لجنة المناقشة، الذين ستثرى ملاحظاتهم وتوجيهاتهم هذه الرسالة، وستكون موضع تقديري واهتمامي.

ولا يفوتني ان أتوجه بالشكر أيضاً لأساتذتي أعضاء هيئة تحكيم أداة الدراسة على توجيهاتهم وآرائهم السديدة، ولأساتذتي في قسم الإدارة العامة وبقية أقسام الجامعة الذين تعلمت منهم الكثير في مرحلة دراستي والى الأستاذ محمد سلامة على الجهد البالغ الذي بذله في تدقيق هذه الرسالة .

والشكر الجزيل للعاملين بالدائرة المالية في أمانة عمان الكبرى، ممثلة بمديرها السيد محمود خليفات، الذين لم يتأخروا عن تقديم العون والمساعدة، وللعاملين بدائرة الحاسوب، وأخص منهم السيد غازي الشبول؛ والسيدة مها الصرايرة؛ كما أشكر المهندسة سراب النجداوي من وزارة المالية، وإلى كل من ساهم وساند في إنجاز هذه الرسالة جزاهم الله جميعاً خير الجزاء، والله ولي التوفيق.

آمنة ماجد عبداللطيف الربيحات

قائمة المحتويات

قائمة الجداول

قائمة الأشكال

قائمة الملاحق

الملخص

أثر التهديدات الأمنية في أمن المعلومات في ضوء تطبيق الحكومة الإلكترونية دراسة ميدانية في عدد من الوزارات الأردنية وأمانة عمان الكبرى

آمنة ماجد الربيحات

جامعة مؤتة2004

هدفت هذه الدراسة إلى التعرف على أثر التهديدات الأمنية بمصادرها الداخلية والخارجية في أمن المعلومات بنتائجها المباشرة وغير المباشرة في ضوء تطبيق الحكومة الإلكترونية على الوزارات المرتبطة بالشبكة الآمنة وهي :(وزارة الاتصالات وتكنولوجيا المعلومات ؛ ووزارة التخطيط ؛ ووزارة المالية ؛ووزارة الصناعة والتجارة ؛ بالإضافة إلى أمانة عمان الكبرى) .

لتحقيق أهداف الدراسة تم تطوير استبانه لجمع البيانات ، شملت على (54) فقرة تم الإجابة عنها وفقاً لمقياس ليكرت الخماسي ، و(14) فقره تمت الإجابة عنها (بنعم) أو (لا) واحتسبت النسب المئوية للإجابة عن كل فقره .

شملت الدراسة على العاملين في قسم الحاسوب، في الوزارات مجتمع الدراسة البالغ عددهم (148) موظفاً، وبعد توزيع الاستبانه على مجتمع الدراسة أعيد منها (115) استبانه وكان صالحاً للتحليل (110) استبانات أي بنسبة (74.3%) من المجتمع الأصلي .استخدمت الرزمة الإحصائية للعلوم الاجتماعية (SPSS) لتحليل بيانات الاستبانة ، كما استخدمت المتوسطات الحسابية والانحرافات المعيارية للإجابة عن أسئلة الدراسة واستخدم تحليل الانحدار لاختبار فرضيات الدراسة .

وقد توصلت الدراسة إلى مجموعة من النتائج كان ابرزها .

1- ثبات صلاحية المتغيرات المستخدمة في قياس أثر التهديدات الأمنية في أمن المعلومات في ضوء تطبيق الحكومة الإلكترونية .

2- توصلت الدراسة إلى وجود أثر ذي دلالة إحصائية للتهديدات الداخلية (التقنية) والتهديدات الخارجية (الكوارث الطبيعية ،والبرمجيات الخبيثة) في النتائج المباشرة وغير المباشرة للتهديدات .

3- توصلت الدراسة الى وجود فروقات ذات دلالة إحصائية لاتجاهات المبحوثين نحو أثر التهديدات الأمنية في أمن المعلومات تعود لمتغيرات مثل (الجنس ،و العمر ، والمؤهل العلمي ، والمسمى الوظيفي) .

وقد خلصت لدراسة الى مجموعه من التوصيات كان من أهمها :

1- ضرورة التنبه إلى خطورة التهديدات الداخلية على أمن المعلومات، لأن حجم الخسارة التي تخلفها كبيراً ، وبخاصة في حالة التهديد البشري لأنه يهدد الماديات والبرمجيات ، ويهز الثقة المتبادلة بين المنظمة والعاملين من جهة ، وبين المنظمة وجمهورها من جهة أخرى .

2- نظراً لأن بناء وإنشاء بنية تحتية وطنية شاملة ومتينة يشكل داعماً أساسي لتوفير الأمان لجميع العمليات الخدماتية والتجارية الإلكترونية، فلا بد من الاهتمام بتجهيز الشبكات والأنظمة المساندة لها لتفادي حدوث أعطال تهز أمن الشبكات واستقرارها.

3- ضرورة توفير سياسة أمنية تحافظ على الموثوقية والخصوصية والتكاملية لكل منظمة تسعى إلى المحافظة على النظام المعلوماتي بأكمله لدعم نجاح الحكومة الإلكترونية.

4-الحذر الشديد أثناء تطبيق الحكومة الإلكترونية من جانب الوزارات المبحوثة ، لأن نجاح أو فشل تجربتها سوف ينعكس على بقية الوزارات عندما يتم تعميم التجربة .

Abstract

The Effect of the Security Threats on the Information Security in the light of applying E-government by Applying a Survey on the Jordanian Ministries and Greater Amman Municipality.

Amnah M. Rbihat
Mu'tah University 2004

This study aims to recognize the effect of the security threats-with both their internal and external sources – on information security with its direct and indirect results by applying the electronic government on the ministries which are associated the safe net–and they are : (Ministry of communication and Information technology, Ministry of Planning Ministry of Finance, Ministry of Industry and Trade and Greater Amman Municipality).

To Achieve the goals of this study, a questionnaire is developed to gather data which includes (54) items which are answered according to Likert Scale and (14) which are answered with "Yes" or " No", and the percentages were calculated to answer each item.

The study includes the employees of (Computer Departments in the ministries. The population of the study is (148) employees. After distributing the questionnaire, (115) of them were turned back and (110) of them were appropriate for analysis (i.e. 74,3% of the original population). The Statistical Parcel of Social Sciences (SPSS) is used to analyze the questionnaire. Also, mathematical averages and standard deviations were used to answer the study. questions and use of regression analysis to test the study hypotheses.

Conclusions of the study:

1- The consistency of variables which are used in measuring the effect of security threats on information security in the light of applying the electronic government.

2- The study found that there was a statistical effect of the internal threats technological and of the external threats (natural disasters and malicious code) in the direct and indirect results of threats.

3- The study found that there are statistical differences of the population's view "the subjects of study" towards the effect of security threats on information security because of many variables such (sex, age, educational certification and job).

Recommendations of the study:

1- It is necessary to pay attention to the dangers of the internal threats on information security that is because it causes great loses, especially with regard to human threat as it affects materials and programming and affects the mutual confidence between the organization and employees from one hand, and the organization and its population from the other.

2- Because building a comprehensive and solid infrastructure is a basic support to make security available for all service, commercial and electronic processes, the nets and support systems must be supplied in a good way in order to avoid the defects which affect the nets security and stability.

3- It is necessary to have a security policy to keep the privacy and the confidence for each organization which aims to take care of information system to support the success of the electronic government.

4- It is necessary to take great care during the application of the electronic government from the ministries which are researched, because the success or the failure of their experiment would be reflected on other ministries if the experiment is generalized.

الفصل الأول

خلفية الدراسة ومشكلتها

المقدمة:

مع تطور الوسائل التكنولوجية، والتوسع في استخدامها في مختلف مناحي الحياة وزيادة أهميتها، برزت الحاجة لأسلوب جديد في إنجاز المعاملات وتقديم الخدمات يتسم بالسرعة، والدقة والإتقان، وغدا أسلوب العمل اليدوي المتبع في الدوائر الحكومية، يقف حائلاً دون تلبية طلبات جميع المواطنين بشكل مرضٍ، وضمن المستوى المقبول بسبب زيادة عدد السكان، وتعاظم مطالبهم، ومحدودية الإمكانيات البشرية وتزايد المنافسة، محليا ودولياً، على تقديم افضل الخدمات للمواطنين بين الیب وأنماط إنجاز المعاملات، وتقديم الخدمات، ومن ثم تدني مستوى الكفاءة، والفاعلية، والإنتاجية، والبطء الشديد بسبب صعوبة الإجراءات، وعدم كفاية الوقت المتاح لإنجاز هذه المعاملات، واقتصار أوقات تقديم الخدمات على الدوام الرسمي فقط، وكثرة القيود على تداول المعلومات، ووضع عدد كبير منها تحت مستويات مختلفة من السرية والكتمان دون ان يكون لذلك دليل واضح ومحدد، واسس علمية تعتمد لهذه الغاية.

لذلك قامت عدد من الدول، ومنها الأردن، بإدخال نظام تقديم الخدمات وإنجاز المعاملات إلكترونياً من خلال اعتماد برنامج الحكومة الإلكترونية بوصفه عنصراً أساسياً لتطوير المجتمعات، وتقدمها، وزيادة قدرتها التنافسية. ففي ظل الثورة الإلكترونية لا يوجد أمام الدول بدائل أخرى سوى اللحاق بركب تكنولوجيا المعلومات والاتصالات، باعتباره مقدمة للتحول نحو تنفيذ برنامج الحكومة الإلكترونية الذي يعني أساساً ربط العاملين والمواطنين في الدولة الواحدة إلكترونياً مع دوائرها ووزاراتها من جهة، وربط هذه الدولة مع الدول الأخرى من جهة أخرى. ويضمن هذا الربط تقديم الخدمات وإنجاز المعاملات بسرعة وفعالية وبشكل مستمر ومستقر مع ضرورة التأكيد على تحقيق خصوصية وحماية للمعلومات المتداولة.

وانطلاقاً من التوجه العالمي نحو العمل بالحكومة الإلكترونية، والارتكاز على مبدأ الشفافية، والحرص على بناء الثقة المتبادلة، والسعي لتحقيق خصوصية في تعاملات المواطنين، فان موضوع أمن المعلومات وسريتها، وخصوصيتها، يعد من دعائم ومتطلبات نجاح الحكومة الإلكترونية. ان لم يكن شرطاً، تمليه علاقة المواطنين بالدولة باعتباره ضماناً لهم. وللمعلومات الهائلة الخاصة بهم التي تحتفظ بها الحكومة وسوف يتم تداولها. فالعمل الحكومي الإلكتروني يعني عملاً طوال اليوم؛ أي خلال (24 ساعة) مما يعني إنجازاً كبيراً ومستوىً متقدماً من الكفاءة والفاعلية التي سيتم الوصول إليها في نهاية رحلة التحول إلى الحكومة الإلكترونية، وذلك الأمر بحاجة إلى مستوىً عالٍ من الحماية والأمن.

لقد أدى تطور تكنولوجيا المعلومات والاتصالات، إلى حدوث تغيرات كبيرة في العمل الحكومي ومتطلباته، وكذلك رافق هذا التطور ظهور مخاطر وأعباء جديدة، إذ لم يكن هناك قلق من حدوث جرائم، أو انتهاكات، أو تهديدات عبر شبكة المعلومات الدولية "الإنترنت" وهي في بدايتها، وذلك لمحدودية مستخدمي هذه الشبكة. لكن مع التوسع في استخدامها، ودخول معظم شرائح المجتمع وطبقاته إلى ركب المستخدمين لها، وتوجه الدول نحو تحويل العمل الحكومي إلى عمل إلكتروني، بدأت تظهر الجرائم بأنواعها وصورها المتعددة؛ فكانت بمنزلة ضاغط أو محرك للمهتمين بتكنولوجيا المعلومات للاهتمام والعناية بتوفير أمن وحماية المعلومات؛ بهدف الوقاية من حدوث جرائم أو انتهاكات أو اعتداءات على حقوق الأشخاص أو الجهات الأخرى.

فالأمن والحماية، كما نعلم، حاجة أساسية لكل فرد، وكيان يحقق له شعوراً بالاستقرار، ويضمن له الاستمرار والنجاح، ويسهم في تقدمه نحو الأمام. وينبغي إلا نغفل ما يعنيه الأمن والحماية للدولة بمجملها، فهو وظيفة رئيسية لها، وواجب عليها، ومسؤولية تقع عليها تجاه رعاياها وممتلكاتها المادية والفكرية. ونظراً لأن الأمن والحماية يعتبر حاجة ووظيفة ومتطلباً للنجاح، حتى إنه غدا – إن جاز التعبير–، موضوع الساعة؛ فإنه جدير بالدراسة والبحث، وحري الاهتمام به على صعيد الحكومة الإلكترونية.

مشكلـة الدراســة

لا جدل في أن التحول في العمل الحكومي من نمط تقليدي إلــى إلكترونــي يرافقه الكثير من الصعوبات والمشاكل على مستويات عدة وفي مجالات متنوعــة، وأحد هذه الصعوبات والمخاوف وأكثرها ضغطاً هو تحقيق الأمنية والخصوصــية لهذا الكم الهائل والحساس من المعلومات والمعاملات التي سيتم نشرها عبر شبكات الحاسوب.

ويتصف موضوع توفير مستويات الأمن والحماية للوقاية من التهديدات بالأهمية والتعقيد البالغين، إذ يؤدي نشر المعلومات أو إفشائها أو عدم تحقيق خصوصيتها إلى حدوث مشكلات مثل: إساءة الاستعمال؛ مع التعرض للتهديد، ومواجهة الخسائر المادية والمعنوية على مستوى الصالح العام والخاص، فضلاً عن حصول شرخ في الثقة بين المتداولين للمعلومات من داخل الجهاز الحكومي وخارجه.

أهـداف الدراســة

اعتماداً على مشكلة الدراسة؛ فإنه ستتم دراسة المشكلة الأمنية بعمق، ومحاولة استقراء حلول لسد الفجوة القائمة حالياً بين مرحلتين فاصلتين، ويتضمن ذلك :

1. تكوين إطار نظري للتعرف على مفاهيم أمن المعلومات والأمنية في كل من العمل الحكومي والإلكتروني والحكومة الإلكترونية وما يــرتبط بهمــا مــن مفاهيم .
2. تحديد متطلبات أمن المعلومات وحمايتها في الحكومة الإلكترونية بما في ذلك الوسائل، والأدوات، والمستلزمات، والإجراءات.
3. الاطلاع على واقع أمن المعلومات في العمل الحكومي بعد المباشرة بتطبيق الحكومة الإلكترونية في عدد من الوزارات بما في ذلـك الأمــن والحمايــة بمستواها الحالي، وتحديد مصادر التهديدات الأمنية ومجالاتها.

4. دراسة أثر مهددات أمن المعلومات وحمايتها على الأمنية في العمل الحكومي في مجالات محددة.
5. معرفة أثر الخصائص الشخصية للمستخدمين والمتعاملين مع الحكومة الإلكترونية على المهددات الأمنية.

أهمية الدراسة

في ضوء تزايد أهمية الحاسوب وبرامجه والتوسع في استخداماتهما في المعاملات التي تتم عبر شبكة المعلومات الدولية "الإنترنت"، برزت الحاجة لتوفير المزيد من الحماية والخصوصية لهذه المعلومات، كما شكل ذلك دافعاً قوياً لإيجاد وسائل أكثر فاعلية لضمان هذه الحماية على المستويين المحلي والعالمي، وبشكل خاص للدول التي تطبق برامج الحكومة الإلكترونية، ومنها المملكة الأردنية الهاشمية، فقد بدأ العمل الحكومي ينتقل من الواقع اليدوي إلى الواقع الإلكتروني بكل ما يتطلبه ذلك من الأنظمة والبرامج والتقنيات والخبرات وما يستتبعه ويرتبط به من التشريعات والقوانين والأنظمة والتعليمات وما سوف يترتب عليه من العقبات والمشكلات. وعليه فقد أصبح لزاماً على المعنيين تهيئة كل مستلزمات النجاح لهذا التحول الكبير. وتأتي قضية توفير الأمن والحماية في مقدمة السياسات والإجراءات التي ينبغي اتخاذها . وتنبثق أهمية هذه الدراسة من الناحية العملية من المعطيات الآتية :

1. أن توفير الأمن والحماية الإلكترونية للعمل الحكومي لا يتوقف عند إعداد برامج حماية كما هو الحال للبرامج التي تستخدمها الشركات الخاصة والجهات ذات العلاقة بالتجارة الإلكترونية، وذلك نظراً لتعدد الأنشطة والفعاليات الحكومية وتعقيدها تبعاً للوزارات والمؤسسات الحكومية المرتبطة بها.
2. أن جانباً من المعلومات والبيانات في العمل الحكومي يحمل قدراً متفاوتاً من السرية وعندما يتم الانتقال إلى العمل الإلكتروني ، فإن ذلك يتطلب سياسات واضحة وإجراءات محددة لحمايتها.
3. أن العمل الحكومي يتسم بتنوع الخصوصيات تبعاً للأطراف المشتركة فيه

المؤسسة الحكومية؛ والمواطن؛ والمجهز؛ والمستثمر.

4. أن التركيز القائم حالياً في مسالة الأمن والحماية من التهديدات هو على الجوانب التقنية البحتة(برامج حماية إلكترونية) دون الاهتمام بالجوانب الأخرى وهي:

أ- الجوانب السلوكية (النفسية؛ والاجتماعية) المتعلقة بالموظف الحكومي الذي سينقل من بيئة العمل اليدوي إلى بيئة العمل الإلكتروني من خلال الحكومة الإلكترونية .

ب-الجوانب التنظيمية التي سوف تترتب على الانتقال من العمل اليدوي إلى العمل الإلكتروني وما يرتبط بذلك من تغيير في الهياكل وعلاقات السلطة والاتصالات واتخاذ القرار .

أما من الناحية الأكاديمية؛ فتنفرد هذه الدراسة – وحسب علم الباحثة- في موضوعها، إذ تخلو المكتبة العربية، وبخاصة على مستوى الدراسات العليا من رسائل تتناول قضية الأمنية في العمل الحكومي الإلكتروني، وبهذا المستوى من الشمول، مما دعا الباحثة لتناول أحد المواضيع الأكثر أهمية من بين القضايا التي يثيرها تطبيق الحكومة الإلكترونية .

الفصل الثاني

الإطار النظري والدراسات السابقة

أولاً : الإطار النظري

أمن المعلومات(المفهوم ،الأهمية ، العناصر ، الوسائل ، الاستراتيجية)

انتشرت مع بروز عصر المعلوماتية مصطلحات ومفاهيم عدة جديدة لها خصوصية متعلقة بالمعلومات والحاسوب. منها أمن الحاسوب الذي تطور عبر السنوات الماضية تطوراً ملحوظاً سريعاً نتيجة لتطور تقانات المعلومات، واستخدام الحواسيب ومردوداتها، حتى أصبح هذا الموضوع من أبرز المواضيع التي تحظى باهتمام عدد من المهتمين بالمعلوماتية، الذين تناولوه بالبحث والدراسة على مستويات مختلفة ومن جوانب وزوايا متعددة عملية، ونظرية.

ونظراً لاختلاف المستويات، وتعدد الزوايا والمداخل التي بحثت في هذا الموضوع، فقد أفضى ذلك كله إلى تنوع المفاهيم التي يتم تداولها حول موضوع أمن المعلومات؛ فبعض الباحثين وصفه أمن الحاسوب، والبعض الآخر أطلق عليه أمن البيانات، وتظل جميع هذه التسميات تصب في مصب واحد هو (أمن المعلومات).

ولكون العصر الذي نعيشه الآن هو عصر المعلوماتية الذي أصبحت فيه المعلومات هي المقياس الذي يحدد مدى قوة المنظمات؛ فمن يمتلك المعلومات هو الذي يمتلك القوة والسلطة، وهو الأجدر بالسيطرة. ويتبدى بوضوح في هذه الأيام الأهمية البالغة للمعلومات، وتزايد قيمتها وما وصل إليه علم الحاسوب من منزلة رفيعة، إذ انتشر تعليم الحاسوب في المدارس، والمعاهد، والجامعات، ويعد علم الحاسوب الآن من العلوم والتخصصات التي تشهد إقبالاً متزايداً على دراستها، وتتوافر لخريجي الحاسوب فرص العمل بسهولة ويسر، بسبب الحاجة إليه وتزايد الاعتماد عليه ، فالحاسب في عصر المعلوماتية هو السلاح الأقوى، والأكثر تأثيراً. أما عن نتاج مخاض ثورة المعلومات، فقد كانت ولادة شبكة المعلومات الدولية "الإنترنت"، والتي يتم من خلالها ربط ملايين المشتركين من مختلف أنحاء العالم الذين يستخدمونها في أي وقت يشاؤون.

لذلك تعد قضية أمن المعلومات قضية مهمة وتزداد أهميتها باستمرار بسبب ما سبق ذكره من تطور وسيطرة المعلوماتية، والحاسب، وثورة الاتصالات وهي القضية الأجدر بالدراسة والبحث في الوقت الحاضر.

الأمن (Security)

وهو من النعم التي منّ الله على عباده بها ، وهو من المطالب النبيلة التي تحاول معظم الشعوب والمجتمعات البشرية جاهدة تحقيقه، وتبذل قصارى جهدها لاستتبابه وانتشاره، وذلك لعلمها أن الأمن من أهم مطالب استقرار الحياة واستمرارها. ولما كان الأمن بهذه المنزلة وبهذه الأهمية في الحياة بين الله -عز وجل- في كتابه الكريم في اكثر من موضع ذكر الأمن وأهميته ودوره في الحياة.

﴿ وإذ جعلنا البيت مثابة للناس وأمناً ﴾ (البقرة ، آية 125).

﴿ الذي أطعمهم من جوع وءآمنهم من خوف ﴾ (قريش، آية 4) .

وعرف الأمن في معجم لسان العرب على أنه "آمن: الأمان والأمانة بمعنى وقد أمنت فأنا أمن وآمنت غير من الأمن والامان . والأمن ضد الخوف" (ابن منظور ، م13، 21).

وكلمة الأمن ذات لدلالة كبيرة، وأهمية بالغة، وتأثير واسع، فهبي تعني باختصار شعور وإحساس بإمكانية استقرار الحياة واستمرارها دون خوف من مواجهة خطر، أو التعرض إلى أي تهديد، فوقوع الطمأنينة والسكينة في النفس، وزوال الخوف هو الأمن .

والأمن حاجة جماعية غير مقتصرة على فئة دون أخرى، فالجميع بحاجة ماسة إليه في نواحي الحياة كافة: السياسية؛ والاقتصادية؛ والاجتماعية؛ والعسكرية؛ والإدارية.

ونظراً لأهمية المعلومات، والحاجة لها لإنجاز أغلب المعاملات والتعاملات، فإنه لابد من توفير حماية لها ضد التهديدات والأخطار التي قد تتعرض لها، ولا بد من ان نسعى لتحقيق أمن معلوماتي على مستوى عالمي.

أمن المعلومات (Information Security)

أما عن تعريف النصف الآخر المكمل لمصطلح أمن المعلومات، فقد عــرف الغريب المعلومات " أنها البيانات التي تجرى عليها معالجــات معينــة، وترتيبهــا، وتنظيمها، وتحليلها بغرض الاستفادة منها، والحصول على نتائج معينة من خــلال استخدامها" . (الغريب ،1994، 81).

وكون الحديث يدور حول المعلومات وأمن المعلومات، والبيانات وأمنها فلابد من التعرف على الوعاء الذي يحوي هذه المصطلحات وهو (تكنولوجيا المعلومات)، إذ يشير المعنى المحدود لتكنولوجيا المعلومات إلى الجانــب التقنــي مــن أنظمــة المعلومات التي تشتمل على الأجزاء الصلبة؛ أي البنية المادية للكمبيوتر، وتعــرف ب(Hardware) والبرامج (Software) وقواعد البيانات (Database) والشبكــــات (Network) وغيرها من الأجزاء، ويشير المعنى الأوسع لتكنولوجيا المعلومات إلى مجموعه من الأنظمة المعلوماتية. والمستخدمين، والإدارة الخاصــــة بمنظمه ما . (Turban & others ,1999،19).

ويتناول مصطلح أمن المعلومات بشكل متكامل، ومترابط دون تجزئة كثيــرة في التعريفات التي أهمها تعريف "عرب" لأمن المعلومات من عــدة زوايــا "أمــن المعلومات من الزاوية الأكاديمية (وهو العلم الذي يبحث في نظريات، واستراتيجيات توفير الحماية من المخاطر التي تهدد المعلومات ، ومن أنشطة الاعتــداء عليهــا)، ومن الزاوية التقنية وهو (الوسائل، والأدوات، والإجراءات اللازم توفيرها لضــمان حماية المعلومات من الأخطار الداخلية والخارجية)، ومن الزاوية القانونية (فإن أمن المعلومات هو محل دراسات وتدابير حمايــة ســرية وســلامة محتــوى، وتــوفر المعلومات، ومكافحة أنشطة الاعتداء عليها، أو استغلال نظمها من ارتكاب الجريمة وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغيــر القانونية التي تستهدف المعلومات ونظمها أي جرائم الحاسوب والإنترنت) (عــرب ، 2002 ،67).

كما عرفه (داود،2000، 23) " بأنه حماية وتأمين كافة الموارد المستخدمة فــي معالجة المعلومات، حيث يتم تأمين المنظمة نفسها، والأفراد العاملين فيها وأجهــزة

الحاسبات المستخدمة فيها، ووسائط المعلومات التي تحتوي على بيانات المنظمة، ويتم ذلك عن طريق اتباع إجراءات، ووسائل حماية عدة تضمن في النهاية سلامة المعلومات وهي الكنز الثمين الذي يجب على المنظمة الحفاظ عليه".

وهناك من يتحدث عن أمن البيانات، ويقصد به " توفير الوسائل والإجراءات التي تحقق الحماية من الأحداث المستقبلية غير المرغوب فيها، وهذه الأحداث تسمى بالتهديدات(Threats) التي تؤدي عادة إلى فقد إحدى جزيئات النظام وفي هذه الحالة يقال انه حدث إخلال بالأمن، ويوجد ثلاثة أنواع من الفقد في النظام هي فقد تكامل النظام، وفقد دقة النظام، وفقد خصوصية النظام (طلبه،د.ت،421)

كما يرى (داود ،2000،216) " بأن أمن البيانات هو تأمين وصول البيانات المطلوبة دون زيادة أو نقصان في الصورة السليمة الصحيحة إلى المستفيد المعني بها دون غيره في الوقت الملائم دون تأخير" .

وعلى الرغم مما نلحظه من تنوع المصطلحات والتعريفات، إلا أنها جميعاً كانت تستهدف وتدور حول ضرورة توفير حماية وسلامة الحاسوب ومردوداته، و تقانات المعلومات من أي اعتداء أو تهديد يخل بهذه السلامة والحماية، وذلك من خلال الالتزام، والتقيد بإجراءات الحماية ووسائلها التي تسعى لتحقيق سلامة المعلومات.

وفي عصر المعلوماتية، فأينما يرد ذكر المعلومات يرد ذكر الحاسوب، فالعلاقة بينهما علاقة تكاملية ، إذ يعتبر الحاسوب مصدر ووسيلة الحصول على المعلومات، وتبويبها، وتصنيفها، وتخزينها، واسترجاعها؛ فأمن الحاسب هو أمن المعلومات التي يحويها ويخزنها، ولم يظهر أمن المعلومات بحالته الراهنة منذ بداية ظهور الحاسب لكنه تدرج في اهتماماته ونطاقه، حيث كان الهم الأكبر والشغل الشاغل في البداية هو تشغيل الأجهزة، وكانت الأمنية تدور حول تحديد الوصول، أو الاطلاع على المعلومات، وذلك من خلال منع الأشخاص الخارجيين من التلاعب أو الاعتداء على الأجهزة، وتوفير البيئة الملائمة والمناخ المناسب، ثم تحول الاهتمام بأمن الحاسوب ذاته، والإجراءات المختلفة لمواقع الحواسيب وقاعاتها، واصبح تركيز الأمنية بعد التوسع في استخدامات الحاسوب وتطبيقاته على البيانات

وحمايتها. أما الآن؛ فقد تحول التركيز في الأمنيــة وتطــور مــن البيانـــات إلـــى المعلومات، وذلك بالاهتمام بالمحافظة على المعلومات، وتكاملها، وموثوقيتها.

أهمية أمن المعلومات (The Importance of Information Security)

ازداد استخدام الحاسوب في إدارة أعمال الأفراد وفي شؤون حياتهم وكلمـا ازداد استخدام الحاسوب والاعتماد عليه ازدادت التهديدات، وظهرت الحاجــة إلـــى حماية البيانات الخاصة به التي قد يؤدي فقدانها، أو تغيرها، أو مجرد الاطلاع عليها إلى نشوء تهديد مباشر على ممتلكات، أو حتى حياة صاحبها.

وتنبع أهمية أمن المعلومات، بالمقام الأول، من كونه موضوعاً يمس شرائح المجتمع كافة على اختلاف أعمار أفرادها، وأعمالهم، واهتماماتهم سواء كان مقــدم الخدمة، أو متلقيها، أو رجل القانون، أو رجــل التشــريع، أو رجــل الأمــن ، أو المدرس، أو الطالب ، أو الرئيس، أو المرؤوس.

كما يتمثل دور المعلومات الأساسي في الحياة الآن وفي عصر المعلوماتيـــة في إنجاز أغلب المعاملات والتعاملات بين الشعوب ، وتقتضي هذه الأهمية البالغـــة للمعلومات ضرورة حمايتها ضماناً لسلامة التعاملات، والمعاملات التي لا تــتم إلا بواسطتها.

ونظراً لان المعلومات هي الهدف والغاية لأغلب السرقات، وفي ضــوء مــا تتعرض له دوماً من تهديدات وخروقات، فانه لا بد من توفير الأمن والحماية لهــذه المعلومات من تلك الأخطار .

وتعد المعلومات في عصر المعلوماتية من اكثر الأسلحة انتشاراً، وفعاليــةً، وتأثيراً، وسرعة، حتى غدت حرب المعلومات في الوقت الحاضر من اشد الحروب وأخطرها؛ وحتى نتقي شر هذه الحرب ، فإنه لا بد من توفير أمن وحمايــة لهــذه المعلومات، وإذا كان محور الاهتمام في بداية عصر المعلومات هو الحصول علــى المعلومات، وتشغيل الأجهزة؛ فإن الهم الأكبر والمشكلة الأهم فــي هــذه المرحلــة المتقدمة من عصر المعلوماتية يتمثلان في كيفية تحقيق الأمن لهذه المعلومات.

عناصر أمن المعلومات والحاسوب .

على الرغم من أن العلاقة بين الحاسوب والمعلومات هي علاقة ارتباطيه؛ إلا أن هناك فرقاً بين عناصر أمن المعلومات وعناصر أمن الحاسوب، وفي كلتا الحالتين؛ فإن هذه العناصر تربطها علاقة تبادلية تكاملية ضمن منظور النظام؛ إذ لكل جزء دوره، وكل جزء يكمل الآخر، وأي خلل في جزء أو عنصر يؤثر في بقية الأجزاء والعناصر الأخرى.

عناصر أمن الحاسوب (داود و المشهداني، 2001 ،(21-30))

ويمكن تصنيف هذه العناصر وفق آلاتي:

أ-أمن الأفراد :

ويتحقق أمن الأفراد من خلال استخدام المحطات الخاصة بمنظومة الحاسوب؛ فهناك عدد كبير من الأشخاص الذين يستفيدون من الحاسوب ويتعاملون معه، فمنهم من هو على قدر من الخبرة والكفاءة، ومنهم من هو من الهواة ويمتلك فضولاً للتعرف، ومنهم من هو داخل العمل، ومنهم من هو خارجه، ومنهم من هو ذو صلاحيات ومخول، ومنهم من هو متطفل، ومنهم الفني، وعامل الصيانة، وموظف التشغيل والنظم،وغيرهم.من خلال استعراض جزء من شريحة المتعاملين مع الحاسوب، نلاحظ أن بعضاً منهم يشكل خط دفاع أول عن أنظمة المعلومات، والبعض الآخر قد يمثل تهديداً أساسياً لأنظمة المعلومات، وأحياناً قد يشكل الشخص نفسه المخول بحماية أمن المعومات، إذا أساء استعمال صلاحياته ولم يتقيد بالإجراءات، خطراً وتهديداً على المعلومات.

ونظراً للدور البالغ والمهم والمؤثر الذي يؤديه الأفراد في توفير أمن المعلومات وحمايتها، فإنه لا بد من وضع جملة من التعليمات والإجراءات المتعلقة بالعاملين وبمن سيتم استقطابهم للعمل، وبالمتعاملين مع الحاسوب، ولا بد أيضاً من بث التوعية في صفوف العاملين والمتعاملين حول قيمة، وأثر وخطورة التهديدات والاختراقات التي يقومون بها، أو التي قد يفكر أحدهم في الإقدام عليها.

ب- أمن الإدارة:

لإعطاء أي قضية وزنها المناسب وخصوصيتها وحقها من الاهتمام والعناية، ينبغي أن تكون هناك إدارة مسؤولة عن هذه القضية تعنى بها، وتنظمها وتخطط لها، وتنسقها، وتوجهها في الاتجاه الصحيح وتحدد الصلاحيات، ونطاق المسؤولية، والمساءلة، وتراقبها، وتواجه الخطأ قبل وقوعه، إن أمكن، أو تخفف من حدته، أو توقفه، وتواجه التهديدات التي يتعرض لها هذا النظام. وبهذا، فإنه لا يمكن إنكار دور إدارة أمن المعلومات في درء الخطر والتهديدات عن المعلومات.

ج- أمن أجهزة الحاسوب والمنظومات الملحقة به.

إن مصدر ووسيلة الحصول على المعلومات هو الحاسوب، والأجهزة، والمعدات التي يعمل بعضها بشكل منفرد، ويعمل بعضها الآخر بشكل شبكة. ونظراً لأن عناصر أمن الحاسوب هي عناصر مترابطة متكاملة يكمل كل منها الآخر كأجزاء النظام الواحد، وحتى يتحقق أمن المعلومات، فإنه لا بد من العناية بهذه الأجهزة، وصيانتها بشكل دوري ومستمر وفي حالات الطوارئ، والحرص على توفير المناخ والبيئة المناسبين من تهوية، وحرارة، ورطوبة، مما يضمن سلامة الحواسيب وحمايتها، وكذلك لا بد من الاستعداد لمواجهة الكوارث الطبيعية من زلازل، وبراكين، وفيضانات، وحروب، وذلك بإعداد خطة الطوارئ.

د- أمن نظم الاتصالات.

يؤدي كل تقدم وتطور في أنظمة ووسائل الاتصالات إلى تطور الحاسبات، وقد أدت سهولة الاتصالات الحالية إلى تسهيل الإمكانيات لمهددي، وسارقي البيانات، إذ أصبح بالإمكان نقل البيانات والملفات عن طريق خطوط الهاتف، أو عن طريق الاتصالات اللاسلكية، وحالياً عن طريق الشبكة الدولية "الإنترنت". وعليه، برزت الحاجة إلى تشفير البيانات المرسلة من مكان إلى آخر، وضرورة وضع إجراءات خاصة بتنظيم، وتحديد طرق الاتصالات بالأجهزة، ونقل البيانات، مع ضرورة مراعاة الحرص والحذر بشأن وسائل الاتصالات الداخلية للمنظمة مثل أسلاك توصيل الشبكات الخاصة بالأجهزة وملحقاتها.

هـ- أمن أنظمة التشغيل والبرمجيات

بعد تحقيق أمن الأجهزة، وهي الجزء الأول من مكونات الحواسيب ، لا بد من السعي لتحقيق الأمن للنصف الآخر من المكونات وهي البرمجيات وأنظمة التشغيل، فقد أصبح من المستحيل اختيار حواسيب ذات أنظمة ولها خصائص أمنية يمكن أن تحقق حماية تامة للبرامج وطرق حفظ كلمات المرور، وطريقة إدارة نظام التشغيل، وأنظمة الاتصالات والبرامج المساعدة، إضافة إلى أهمية توفير أمن للأنظمة العاملة على هذه الأجهزة وبياناتها، وذلك من خلال احتواء البرمجيات على وسائل تحديد عدد المستخدمين لنظام معين، أو طرق الاطلاع، أو تعديل بياناتها، وكما انه لا بد من الاهتمام بوضع الإجراءات المناسبة أثناء كتابة الأنظمة داخل المنظمة لضمان عدم ترك المجال مفتوحاً أمام المبرمج للاطلاع على بعض البيانات الخاصة بالمنظمة، مع ضرورة مراعاة الحذر والاحتياط من تسرب، أو دخول البرامج الخبيثة(الفيروسات) إلى داخل الأجهزة، وذلك بالتأكد من مصدر البرمجيات وفحصها بشكل دوري.

عناصر أمن المعلومات (عرب، 2002، 68) .

وتتضمن هذه العناصر ما يلي:

أ-"السرية أو الموثوقية (CONFIDENTIALITY)وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك" .

ب-"التكاملية وسلامة المحتوى (INTEGRITY) التأكد من ان محتوى المعلومات صحيح ولم يتم تعديله، أو العبث به وبشكل خاص لن يتم تدمير المحتوى، أو تغييره، أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات، أو عن طريق تدخل غير مشروع".

ج-"استمرارية توفر المعلومات (AVAILABILITY) التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات لن يتعرض إلى منع استخدامه أو دخوله إليها".

د-"عدم إنكار التصرف المرتبط بالمعلومات ممن قام به(Non repudiation) ويقصد ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو إنكار انه هو الذي قام بهذا التصرف بحيث تتوفر قدرة إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين".

الوسائل المستخدمة في سرقة المعلومات

إن الوسائل المستخدمة في سرقة المعلومات كثيرة ومتعددة وهي في تزايد مستمر وتتطور مع كل خطوة تقدم في مجال المعلوماتية، ويتم هذا الانتهاك وهذه السرقات من جانب أشخاص مخولين، وغير مخولين باستخدام النظام المعلوماتي، واهم هذه الأساليب:

أ-"استخدام المحطات الطرفية أو العقد التابعة للمنظومة وعن طريق استخدام كلمات المرور(كلمة السر) للوصول إلى بيانات النظام".

ب-" استخدام أجهزة التنصت وما يماثلها على أجهزة المنظومة".

ج-"استخدام أسلوب التنصت، وبخاصة ضمن خطوط الاتصالات التي تربط عناصر الشبكة والمحطات الطرفية البعيدة عن مركز المنظومة".

د-"الحصول على مخرجات النظام بشكل غير قانوني، أو بسبب إهمال المخولين باستخدام النظام".

هـ-الدخول غير الشرعي إلى مكتبة الأشرطة والأقراص الممغنطة للمنظومة بغرض الحصول على المعلومات المخزونة فيها". :(داود و المشهداني ،2001، 71)

إدارة أمن المعلومات

حتى تأخذ أي قضية الخصوصية والأهمية والعناية الكافية، ينبغي توافر إدارة مسؤولة عن هذه القضية تعنى بها، وتنظمها، وتخطط لها، وتنسقها، وتوجهها، وتراقبها، وتصحح الخطأ، وتواجه الأخطار، والتهديدات التي تتعرض لها المعلومات، وتكون هذه الإدارة مرتبطة مع من يفيد النظام المعلوماتي ويستفيد منه.

وكون وظيفة أمن المعلومات مسؤولة عن توفير أمن المعلومات، وحمايتها، وسلامتها عن طريق تطوير، وتنفيذ، وصيانة برامج أمن المعلومات المخصصة لأغراض حماية تكامل المعلومات وسريتها، وموثوقيتها، وإعداد الخطط لمواجهة التهديدات الواقعة على المعلومات، والمهددة لأمنيتها. إذاً، لا بد من وجود إدارة مسؤولة عن أمن المعلومات من منطلق أن الوظائف الإدارية، بشكل عام، تشتمل على التخطيط، والتنظيم، والتنسيق ، والتوجيه والرقابة. وعليه، ونظراً للأهمية البالغة للمعلومات، وضرورة توفير الأمنية لها؛ فإن الحاجة تستدعي وجود إدارة مسؤولة عن تحقيق أمنية المعلومات وسلامتها.

وتؤكد التطورات التكنولوجية الملحوظة أهمية وجود إدارة أمن معلومات باعتبارها أداة مسؤولة عن تحقيق الأمنية، وتتابع، وتراقب، وتطور الخطط، وتبث الوعي حول أهمية أمن المعلومات، وخطورة اختراق الأمنية، وكذلك تكون مكلفة بتطوير إجراءات تأمين الحاسبات، واستخدام التقنيات المضادة لأغراض الحماية، وموكول إليها إصدار تشريعات خاصة تتيح حماية المعلومات وأمنها، وتردع كل من يحاول انتهاك أمنية، وسلامة وكمال، وموثوقية، وخصوصية المعلومات.

لقد اقتصرت قضية توفير أمنية المعلومات وحمايتها في البداية على استخدام برامج حماية الفيروسات، أو تركيب الجدار الناري فقط. وكان هذا مجدياً قبل ظهور الشبكة العالمية "الإنترنت" عندما كان يقتصر استخدام الحواسيب على البرامج الشخصية، لكن اليوم لم تعد هذه الوسائل فعالة، وكافية لوحدها، وأصبح أمن المعلومات علماً يدرس بشكل مستقل بذاته يهم العمل التجاري والحكومي. وتعتمد أغلب دول العالم على وجود إدارة أمن، وقد عرفت إدارة الأمن بأنها "عملية الحفاظ على مستوى مرتفع، ومستقر من أمن المعلومات والخدمات المعلوماتية في مختلف قطاعات الشركة وإدارة الإجراءات المتعلقة بهذا الأمن بالطريقة المثلى التي تحافظ على استقراره" (سالم ، 2000، 55).

وتشتمل الإدارة الأمنية على أمن الحاسوب الذي يضم العاملين في المنظمة، والتطبيقات، والبرامج التي يحتويها الكمبيوتر، وكذلك أمن الشبكات بنوعيها المحلية والعالمية ، بالإضافة إلى تحقيق الأمن الفيزيائي لأمن الكمبيوتر وأمن

الشبكات ضد الكوارث، والسرقات، والحرائق، والأخطار الطارئة سواء كانت الأخطار المعلوماتية،مثل: الاختراق؛ والفيروسات، أو الفيزيائية،مثل: الحرائق؛ والكوارث؛ والسرقات.

والمسؤول الأول عن إدارة أمن المعلومات هو الإدارة العليا ممثلة بالمدير. ولنجاح هذه الإدارة لا بد من إشراك العاملين في المنظمة في كل المستويات، وهذا ما يتحقق من خلال إشراكهم في دورات وندوات التوعية على الأقل، ولا يوجد شك في الحاجة إلى مستشارين في مجال الأمنية ومتخصصين، ولا سيما في الدول النامية لحداثة العلم والتخصص فيها.

استراتيجية أمن المعلومات

يتطلب إعداد استراتيجيات أمن المعلومات وحمايتها أو خطة الحماية القيام مسبقاً بتحديد البيانات والمعلومات التي يراد حمايتها، إذ يتم من خلال تصنيف المعلومات تحديد ماهية المعلومات السرية، والسرية جداً، وغير السرية التي يستطيع أي شخص الاطلاع عليها. وبناءً على تصنيف المعلومات من ناحية سريتها بالإمكان التنبؤ بماهية التهديدات التي قد تتعرض لها المعلومات، وفي ضوء معرفة هذه التهديدات يمكن مبدئياً وضع التصورات وتحديد وسائل مواجهتها، وهناك حقيقة لا يمكن إغفالها، أو تجاهلها تتمثل في أنه لا يوجد أمن مطلق، إذ يجب التهيؤ والاستعداد لمواجهة هذه المخاطر والتهديدات بدءاً من إيصال الحاسوب بالمصدر الكهربائي، ويكون ذلك من خلال وضع السياسات والاستراتيجيات الأمنية، واستحداث وسائل أمن المعلومات وحمايتها.

ويعد الإنسان، سواء كان مستخدماً، أو فنياً، أو مشغلاً، نقطة الارتكاز في نجاح أو فشل استراتيجية أمن المعلومات وحمايتها، فإدراك الإنسان ووعيه بحدود صلاحياته وخطورة قيامه بانتهاك الأمنية، ومدى المساءلة المترتبة على قيامه بذلك العمل، وحجم الدمار المتحقق جراء هذا الانتهاك، وجسامة المسؤولية الملقاة على كاهله، وعظم الفائدة العائدة على التزامه وتقيده بالقوانين ، والإجراءات، والتعليمات

المعمول بها في هذا المجال ، كلها عوامل تشكل نقطة الانطلاق في مسيرة تحقيق الأمن والحماية المعلوماتية.

وأحد مسؤوليات إدارة أمن المعلومات هو بناء استراتيجية واضحة لأمن المعلومات حتى يتم الالتزام والتقيد بها من العاملين والمتعاملين بالحاسوب وتقنياته. وقد عرفت استراتيجية أمن المعلومات أنها " مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية، ومع المعلومات داخل المنظمة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها" (عرب ، 2002، 176).

ويسهم إشراك العاملين في المنظمة بمستوياتهم الوظيفية كافة في إعداد الإستراتيجية وتنفيذها في تحقيقها لأهدافها المرجوة، وتوفير الدعم الكامل لها من جميع المستويات وفي مراحلها المتعددة.

وتتوافر لكل استراتيجية جملة من الأهداف، وأهم أهداف استراتيجية أمن المعلومات. (عرب ، 2002،177)

أ-تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الحاسوب والشبكات، وكذلك حماية المعلومات بأشكالها كافة وفي مراحل إدخالها، ومعالجتها، وخزنها، ونقلها واعادة استرجاعها.

ب-تحديد الآلية الإلكترونية التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة على كل من له علاقة بالمعلومات، ونظمها، وتحديد المسؤوليات عند حصول الخطر.

ج-بيان الإجراءات المتبعة لتجاوز التهديدات، والمخاطر، والتعامل معها وتحديد الجهات المنوط بها القيام بذلك.

ويفترض أن تنطلق استراتيجية أمن المعلومات أساساً من تحديد المخاطر، وأغراض الحماية، ومواطنها، وأنماط الحماية اللازمة، والإجراءات الوقائية ضد المخاطر، مع الأخذ بالاعتبار الاحتياجات المتباينة لكل منظمة عن الأخرى.

وسائل الأمن والحماية المعلوماتية

يشاهد في كل يوم من أيام عصر المعلوماتية تطور جديد في مجال التقنيات والبرمجيات، ويواجه كل تطور تهديداً يستدعي إيجاد وسيلة مقاومته أو حمايته للتصدي له.

وينطلق بناء وسائل أمن وحماية فاعلة من تحديد احتياجات المنظمة الأمنية، وأغراض الأمن فيها، وتصنيف المعلومات فيها ليتسنى تقديم وسائل تناسب الإمكانيات المادية للمنظمة وتتواءم معها، وتراعي الاختلاف في احتياجات المنظمات الأخرى.

ويشكل حسن اختيار الأفراد المؤهلين علمياً وذوي الخبرات العملية الخطوة الأولى نحو تحقيق الأمنية داخل المنظمة. ولا يخفى أيضاً الدور الإيجابي لوعي الأفراد وإدراكهم لأهمية الأمنية ومساهمتها في نجاح العمل الإلكتروني واستمراره، وما يمثله هذا الدور من ركيزة أساسية لتنفيذ السياسات الأمنية المقترحة. وهناك أيضاً عدد من العوامل التي تستحق الاهتمام والعناية يقف في مقدمتها التزام الأفراد بالتعليمات، والقواعد، والأسس، والقوانين، والتقيد بأخلاقيات استخدام التقنية، وبناء ثقافة أمن لدى العاملين ترسخ في أذهانهم، وتصبح جزءاً من شخصيتهم.

ويزداد يوماً بعد آخر عدد من الأفراد المستفيدين والراغبين في الحصول على وسائل الأمن والحماية، الأمر الذي أدى إلى تنوع هذه الوسائل. ومن أبرزها الوسائل الفنية، وغير الفنية، والمعايير الحيوية.

أولاً: الوسائل الفنية وتتمثل هذه الوسائل في:

1-توفير برمجيات ضبط الوصول أو الولوج للمعلومات، إذ تعتبر هذه المعدات الأمنية بالغة الأهمية، وذات اثر واضح في منع أخطاء الأفراد، أو حدوث حذف أو تغيير بسبب سوء تصرف العاملين سواء كان ذلك عن قصد أو بدونه، وتساعد هذه البرمجيات أيضاً في الحد من وصول المستخدم للمعلومات ومصادر النظام وبرامجه من خلال مراقبة عملياته، وإصدار تنبيه وإنذار عند حدوث أي خرق وتراقب فعاليات المستخدم وتنبه وتنذر عند حدوث الخرق.

2-التشفير، ويتضمن استخدام خوارزميات رياضية أو أجهزة ومعدات لغـرض تشفير تناقل المعلومات أو تشفير الملفات.

3-حماية بوابة الدخول للنظام المعلوماتي المحوسب.

4-اتباع الأساليب التي تتأكد من موثوقية الرسائل مع أنظمة المعلومات.

5-الفيروسات وسبل وأساليب الحماية منها. (البياتي ، 1996 ،(43-44)).

ثانياً: الوسائل غير الفنية:

وتشتمل على الأمور المادية والإدارية، مثل: وضـع الأسـاليب، وإعداد الخطط وبث التوعية الأمنية في صفوف الأفراد، ووضع معـايير وضوابط أمنية للموقع والأفراد؛ فالإجراءات المادية تركز على الأساليب، والاستعدادات الاضطرارية وأساليب ضبط الوصـول لمواقـع الأجهـزة والوثائق للعاملين والخارجين غير المخولين بالدخول إليها. (البيـاتي ، 1996 ،(43-44)).

ثالثاً: المعايير الحيوية:(المفهوم،طريقة العمل،أهم هذه المعايير)(للزعبي،2002 ،(3-6)).

وهي من الوسائل الأمنية الحديثة التـي تسـتخدمها المؤسسـات لتخويـل مستخدميها الدخول إلى أنظمتها المختلفة أو تجارتها الإلكترونية. وتعـد المعـايير الحيوية من أبرز القضايا التي يزداد الاهتمام بها يوماً بعد يوم. وتعـرف المعـايير الحيوية للأشخاص" بأنها صفات مرتبطة بالشخص نفسه قـد تكون جزءاً من أجزاء جسمه، أو جزءاً من سلوكه، وتهدف إلى التعرف بالشخص، ومن الأشياء التي تعتبر جزءاً من جسمه: بصمات الأصابع، وشكل راحة اليد، قزحية العين، قرنية العـين، شكل الوجه؛ أما أجزاء سلوكه فهي: الصوت وقد يكون جزء من سـلوكه التوقيـع وسرعة استخدام لوحة المفاتيح ونموذج استخدام لوحة المفاتيح" .

وتعد هذه المعايير من أقوى أنواع التخويل وأكثرهـا أمانـاً، إذ لا يمكـن استعارتها، أو سرقتها، أو نسيانها، كما أنها استخدمت لتنظيم حركة الـدخول إلـى المواقع والمباني؛ لأنها لا تعتمد في تدقيقها على أشخاص، وهي مجدية فـي حـال وجود أعداد كبيرة من المستخدمين، والمعايير الحيوية موجودة منذ زمن، ولكنهـا

مستخدمة للأشغال ذات السرية، ودرجة الأمان العالية جداً وهي مازالت في مراحل التطور.

طريقة عمل المعايير الحيوية

بعد القيام بتحديد نوع المعيار الحيوي واعتماده واستخدامه، يتم تخزينه على الملف المحلي أو الملف المركزي، أو على أي وسيلة تخزين متحركة، مثل البطاقات الذكية. وعند حصول أي محاولة من الشخص للدخول إلى الشبكة يتم أولاً التقاط المعيار الحيوي، ومن ثم أخذه وتخزينه لمقارنته مع ما هو مخزن أصلاً، وفي حال حدوث التطابق يتم حصول الشخص على الموافقة بالدخول إلى النظام مع تسجيل تاريخ الدخول، ووقته، ومكانه.

أهم هذه المعايير:

أ-**بصمات الأصابع:** وهي من النعم التي ميز الله بها كل إنسان عن الآخر، وتستخدم البصمات لتحقيق الأمنية، ويجري التعامل معها بأساليب مختلفة منها: مقارنة البصمات مع بعضها البعض، أو استخدام الموجات فوق الصوتية، وهناك بعض الأنظمة لمعرفة، إذا كانت البصمة من إصبع حي أم ميت. وتعد البصمات نظاماً أمنياً للمعلومات، قليل التكاليف ومناسباً لتدريب الأشخاص عليه من داخل المنظمات.

ب-**شكل اليد:** تستخدم اليد بوصفها أداة حيوية لتحقيق أمن المعلومات من خلال تحليل وقياسات شكلها. ويتميز هذا النوع من المعايير بسهولة الاستخدام، ومناسبته للمواقع ذات الأعداد الكبيرة من المستخدمين، أو عندما يكون استخدام النظام محدوداً، أو في حال عدم تقيد المستخدمين بالأنظمة والتعليمات.أما فيما يتعلق بمستوى الدقة؛ فيمكن أن تكون هذه الدقة عالية إذا رغب صاحب النظام في ذلك. وهذا المعيار شائع الاستخدام في نظام مراقبة الدوام، ويتميز بسهولة ربطه مع الأنظمة الأخرى.

ج-**قرنية العين:** يتضمن هذا المعيار تحليل الأوعية الدموية الموجودة خلف العين. ويتطلب ذلك استخدام ضوء خافت لكي يتم مسح القرنية، ويعد هذا المعيار

عالي الدقة خصوصاً أنه يحتاج إلى تركيز نظر المستخدم عند توجيهه إلى نقطة محـــددة في الجهاز الموجود أمامه، وهو غير ملائم في حالات وجود النظارات على العيون.

د-**قزحـــية العين:** يرتكز هذا المعيار على اختبار المواصفات في اللون الموجود في حلقة العين التي تحيط بالبؤبؤ، وهو يستخدم كاميرا عادية، ولا يتطلب هذا المعيـــار وجود المستخدم قريباً جداً من الكاميرا.

هـ-**الوجـــــــــه:** يتطلب هذا المعيار دراسة مواصفات الوجه، ووجود كــاميرا رقمية لإيجاد صورة للوجه من أجل تخويل المستخدم بالدخول إلى النظام، ويتميــز هذا النوع بحاجته لاستخدام أجهزة معينة غيــر متــوفرة فــي أجهــزة الحاســبات الشخصية.

و-**التــــــوقيــــــع:** يتم تدقيق التوقيع بتحليل كيفية قيام المستخدم بتوقيع اسمه مثل: سرعة التوقيع، ومقدار الضبط ، وشكل التوقيع، وهذا المعيار يعتبر دقيقاً بنسبة تفوق المتوسط مع إمكانية ربطه بالمعايير الأخرى.

ي-**الصــــــــوت:** وهو لا يعتمد على تمييز الصوت بل على تحويله إلى طباعــة، حيث تقوم تكنولوجيا معقدة بتحويل الصوت إلى كتابة، ولا يحتاج هذا المعيار إلـــى تكاليف إضافية نظراً لاحتواء كل الحواسيب الشخصية على ميكرفون وهـــي تقنيـــة معقدة يؤخذ عليها إمكانية حصول إزعاج وتشويش يؤثران علـــى نقــاء الصــوت ونوعيته.

ويكمن المبرر حول سبب انتشار استخدام أنظمة الحماية وأمن المعلومـــات للمعايير الحيوية في ما توفره هذه المعايير من إمكانيـــات التأكـــد مـــن شخصـــية المستخدم، والتعرف على شخصيته، إذ يقوم النظام بالبحث في قاعدة البيانات عـــن هوية المستخدم. وتعتمد استخدام أنظمة المعايير الحيوية على ماهية الأنظمة المراد حمايتها، وعلى ماهية الأشخاص المراد حماية الأنظمة منهم.

ومهما بلغت هذه الوسائل والمعايير من تنوع وتشعب، فانه كل يوم يظهـــر تهديد جديد بحاجة إلى وسيلة حماية ومقاومة له. وهذه الوسائل ليست علاجاً سحرياً يقف في وجه التهديدات والخروقات، لكنه يوقف، قدر الإمكـــان ، أو يخفـــف مـــن أضرار التهديدات، والخروقات، والنتائج الأمنية المترتبة عليهما.

واقع وطموحات أمن المعلومات على مستوى العالم بشكل عام ، والأردن بشكل خاص.

لقد كانت الولايات المتحدة الأمريكية أول دولة طورت نظاماً لتصنيف أمن أنظمة الحواسيب في عام (1983) ثم لحقتها ألمانيا عام (1989)، حيث أصدرت وكالة أمن المعلومات نظامها الخاص بتقييم أمن الحواسيب (البياتي ، 1996، 39).

ولا تقتصر اهتمامات دول العالم الأمنية على ذلك فقط، بل شمل ذلك أيضاً عدداً من المؤسسات والشركات المهتمة بالأمنية في العالم، فهناك تحالف برامج الحاسوب التجارية(Business Software Alliance, BSA)، وجمعية وطنية لأمن الحاسوب (A C S A) في الولايات المتحدة الأمريكية. كما يوجد هناك تزايد في بيع البرامج والمعدات الأمنية في أمريكا بنسبة (40%) كل سنة (سويدان ، 1997،20).

وفيما يتعلق بالوعي بأمن المعلومات والبيانات في العالم، فقد بينت دراسة قام بها فريق من"مجموعة خدمات الحاسوب"(Data Pro)عام (1991) شملت عدد من رجال الأعمال، والشركات، والمؤسسات الحكومية الأمريكية، أن (90%) من المؤسسات الحكومية لديها خطة أو سياسة أمنية، و(7%) لديها مشروع أمني، و (2.5%) لا توجد خطط لديها. وعام (1992) كانت خسائر ميزانية الحكومة الأمريكية 4 بلايين دولار بسبب خرق المفاهيم الأمنية للحاسوب (ابو عياش، 1997،16).

أما بخصوص حالة الأردن في مجال أمن المعلومات، حيث أظهرت "دراسة لمركز المعلومات الوطني عام (1994) " أن (61.7%) من المعلومات في القطاع الحكومي يتم الاحتفاظ بها ومعالجتها بوساطة الحاسوب، وان (26.2%) من هذه المعلومات يتم تحديثها بشكل دوري دون تحديد مدة دورية للتحديث، في حين يحتفظ القطاع الخاص في الأردن بما نسبته (47%) من معلوماته بوساطة الحاسوب، ويتم تحديث (38%) منها بشكل يومي،و(7%) منها بشكل سنوي،و(6%) بشكل فصلي،و(5%) بشكل شهري، (1.5%) بشكل أسبوعي، أما البقية، فهي دون سياسة واضحة للتحديث، وان نسبة المؤسسات التي يتوافر لديها أجهزة حواسيب بلغت (86.7%) من مجموع مؤسسات القطاع العام، منها (58%) تستخدم أجهزة شخصية، و(16%) أجهزة صغيرة، و(18%) أجهزة متوسطة، و(8%) أجهزة

كبيرة؛ واظهرت الدراسة أن ما نسبته (43.7%) من مجموع مؤسسات القطاع الخاص يتوافر لديها أجهزة حواسيب منها (88.5%) أجهزة شخصية صغيرة، و (2%) أجهزة متوسطة، و(1%) أجهزة كبيرة.(ابو عياش ، 1997،(16-17)).

ولقد حقق مركز المعلومات الوطني في الأردن إنجازاً كان له صدى في ميدان أمن المعلومات تمثل في إعداد السياسة العامة لنظام أمن وحماية المعلومات عام (1998)، وكان ذلك خير شاهد على اهتمام الأردن وتقدمه في هذا المجال. وهدفت هذه السياسة إلى التأكد من حماية كل المعلومات المصنفة، والمحددة والممتلكات الحكومية، وحدد في سياق هذه السياسة متطلبات السياسة والتطبيق، والإجراءات الوقائية، والانتهاكات، والمخالفات، وعقوباتها، وتم وضع أسس لتصنيف المعلومات وسريتها، وحدد مفهوم نظم الحماية والخصوصية، ومعايير كل من الأمن المادي وإرسال وشحن المعلومات المصنفة والمحددة، ومعايير أمن وحماية الاتصالات وتكنولوجيا المعلومات.

أما على صعيد برنامج الحكومة الإلكترونية الأردني، فقد بدأت وزارة الاتصالات وتكنولوجيا المعلومات في شهر شباط من عام (2003) بتنفيذ الشبكة الآمنة، إذ تم ربط (6) مؤسسات حكومية كمرحلة تجريبية، وهذه المؤسسات هي" رئاسة الوزراء، و وزارة الصناعة والتجارة؛ و وزارة التخطيط؛ وأمانة عمان الكبرى؛ و وزارة المالية؛ و وزارة الاتصالات" وفي مرحلة لاحقة سيتم تحديد المؤسسات المقرر ربطها حتى نهاية العام(2003)، ويتوقع أن تكون بين(15-30) مؤسسة حكومية(جريدة الدستور، 2003،29).

الأمنية والعمل الحكومي اليدوي والإلكتروني.

أولاً:العمل الحكومي اليدوي" التقليدي" المفهوم التقليدي .

يتسم إنجاز العمل الحكومي يدوياً بكثرة العمل الورقي وتراكم الملفات التي تشغل مساحات واسعة في المكاتب، ويستغرق ذلك العمل وقتاً طويلاً وإجراءات متعددة تتميز بالتعقيد والروتينية، وتحتاج إلى عدد كبير من الموظفين لإنجاز

المعاملة، ولا يعود ذلك لصعوبة العمل، ولكن لارتفاع درجة التعقيد فيه وتشعب إجراءاته.

ولم يكن توفير الأمنية لهذه المعلومات التي تحتويها تلك الأوراق أمراً معقداً إذ كانت الإجراءات الأمنية للمعلومات تنحصر في وضع السجلات والملفات في أدراج، وتأمين هذه الأدراج أو الصناديق بالأقفال أو بالمفاتيح، أو بعدم إعطاء المعاملة باليد للمواطن، وعدم السماح له بالاطلاع عليها، وذلك بتوكيل المراسل أو الموظف المعني بمتابعة تنقل المعاملة حتى النهاية، أو أن يتم وضعها في مغلف مغلق حرصاً على المعلومات التي يحتويها.

وكثيراً ما كانت تؤثر على أمنية المعلومات وسريتها صلة القرابة والمجاملات والوساطات، إذ بمجرد معرفتك للموظف المسؤول أو حتى المراسل الموجود في المنظمة تتمكن من الحصول، ولو على جزء بسيط، من المعلومات التي على الأغلب تكون سرية.

ولا تستطيع حصر الخطر والتهديد الذي يواجه الملفات والسجلات بسرقة المعلومات والاطلاع عليها، إذ يتعرض أمن الوثائق إلى أخطار أخرى مثل: الحريق، والكوارث الطبيعية؛ والحروب؛ وكذلك سوء حفظ هذه الوثائق وتقادمها. لذلك لا بد من العناية بها لأهميتها، ومواجهة أنواع التهديد كافة التي من الممكن أن تتعرض لها.

أمن الوثائق

وهو من أبرز المواضيع التي تشغل بال العاملين في مجال الأرشفة وحفظ الوثائق ومواد الكتابة والأوعية التي تحمل المعلومات سواء كانت سجلات أو ملفات أم أفلام "ميكروفيلم" أو غيرها، والمقصود بالوثائق الأرشيفية "هي الأوراق التي تنشأ أثناء تأدية عمل من أي نوع وكانت جزء من هذا العمل لذلك حفظت لدى الأشخاص المسؤولين عن تصريف هذه الأعمال للرجوع إليها". وقد تكون هذه المعلومات مرتبطة بعمل حكومي أو غير حكومي لأشخاص أو جمعيات أو هيئات، وتعد بمثابة أدلة مادية للعمل المنجز .

وأنواع الوثائق كثيرة منها الرسمي وغير الرسمي العام والخاص من خطابات ومذكرات، وتقارير، ودراسات، ونشرات، وقرارات، وأوامر، ومحاضرات، واجتماعات فهي تمثل جزءاً من التاريخ في الماضي والحاضر لما تحتويه من معلومات مهمة وثرية. ونظراً لأهمية هذه المعلومات التي تحتويها الوثائق، فلا بد من الحرص عليها، وحمايتها، وتوفير الأمن لجميع أنواع وأشكال هذه الوثائق والأوراق حتى نضمن وصول المعلومات من جيل لآخر. (حمودة،د.ت،(5-6))

مجالات أمن الوثائق :(حمودة،د.ت،(7-16)).

1) أمن المعلومات السرية:

تختلف أهمية الوثائق وما تحتويه من معلومات عن بعضها البعض في المنظمة نفسها ومن منظمة إلى أخرى، وكذلك تختلف مستلزمات حماية سرية هذه المعلومات ويؤدي اطلاع الأشخاص من غير المخولين وغير المعنيين على المعلومات إلى إلحاق الضرر بشخص ما أو جهة ما بإفشاء أسرار ذلك الشخص أو تلك الجهة. وعليه ينبغي اتخاذ الإجراءات التي تحصن وتحمي هذه الوثائق السرية ويصبح الاطلاع عليها حكراً على المختصين والمصرح لهم وذلك من خلال تحديد الموظف المسؤول عن درجة سرية هذه الوثائق وما تحويه من معلومات على المغلف الخاص بالوثائق، وتتدرج السرية بين :-

أ-سري:ويختص بالأوراق التي تحتوي معلومات عن الأفراد مثل: التحقيقات، والتقارير السرية؛ أو الإحصائيات؛ أو أسرار العمل التي تتصل بمصالح الجمهور مثل: السجل، وصندوق التوفير.

ب- سري جداً :وتتعلق بالأوراق التي تحتوي معلومات خاصة بالجهات أو الهيئات أو المؤسسات، ويؤدي إفشاؤها إلى إلحاق الضرر بالصالح العام مثل المعلومات المتعلقة بالعطاءات والمناقصات.

ج- سري للغاية:ويختص بالأوراق التي تحتوي على معلومات خاصة بالصالح العام والدولة مثل: التقارير العسكرية، والمسائل الحربية، ومعلومات عن أفراد القوات المسلحة والأسلحة، والمسائل الدبلوماسية والسياسية الخارجية لدولة.

د-محظور الاطلاع عليه: وتكتب هذه العبارة على الأوراق التي تتعلق بنظام أو مشروع أو خطة عسكرية أو مباحثات ومفاوضات دبلوماسية غير معلنة.

ومهما كان مستوى سرية المعلومات، فإنه من الملحوظ أن هنالك ضرراً متحققاً جراء إخلال أمنية هذه الوثائق لذلك لا بد من الحرص على أمن المعلومات وسريتها لأنه لو لم يكن هنالك ضرر جسيم متحقق من إفشاء الأسرار لكانت هذه المعلومات معلنة.

2) الأمن الذاتي، والأمن الصناعي:

الأمن الذاتي " هو التصرف النابع من ذات الإنسان والذي يؤدي بعض الأحيان في حال عدم مراعاته إلى إحداث الأضرار البالغة في الأوراق أو مواد الإنتاج الأخرى التي يعمل بها نتيجة عدم التزامه بمراعاة المحظورات"(حموده،د.ت،9) ومن أهم هذه المحظورات، وأكثرها تأثيراً على الأمن المادي للوثائق:

أ-التدخين: و يعد سبباً رئيسياً في حدوث الحريق، ومن ثم إتلاف ما يحويه المكان من ملفات، أو أوراق، أو وثائق.

ب-تناول المشروبات والأطعمة: حيث يؤدي تناول المشروبات داخل مكاتب العمل إلى إمكانية تعرض هذه المكاتب بما تحتويه من سجلات و أوراق إلى خطر سقوط المشروبات على الوثائق وإتلافها، وتأخير إنجاز المعاملة إلى حين استخراج وثيقة بديلة عن الوثيقة الأصلية، كما يعمل تراكم بقايا الأطعمة في المكاتب وأدراج المكاتب على إيجاد بيئة مناسبة لتكاثر الحشرات والفئران التي تؤدي بدورها إلى تلف الوثائق.

الأمن الصناعي : "وهو ما يوفره الإنسان من وسائل للمحافظة على سلامة وامن وسائل الإنتاج في المنظمات أو على أمن وسلامة الأوراق في دور الوثائق وأقسام الأرشيف والمخازن والمكتبات بما يضمن سلامة العمل والعاملين على حد سواء" .

ويتحقق الأمن الصناعي من خلال الالتزام بوسائل المحافظة على سلامة وأمن وسائل الإنتاج التالية:

أ-الحرص على توفير أماكن صحية ذات تهوية جيدة بعيدة عن مناطق المياه وتسربها وبعيدة عن صناديق توزيع الكهرباء الرئيسية خوفاً من حدوث حرائق.

ب-تزويد غرف حفظ الوثائق وأقسام الأرشيف بأجهزة الإنذار ضد الحريق والسرقة وغيرها .

ج-توفير خزائن حديدية لحفظ الوثائق السرية والمهمة في حال حدوث اية كارثة طبيعية.

د-الحرص على قطع التيار الكهربائي عن المباني بعد انتهاء العمل حتى لا يحدث تماس كهربائي.

3) الأمن من أخطار الحروب:

تحتفظ كل منظمة بوثائق ومستندات هامة في غرف حفظ خاصة، منها ما يحفظ إلى مدة معينة، ومنها ما يحفظ بشكل مستديم. ونظراً لأهمية هذه المستندات، فإنه لا بد من الحرص عليها، وأخذ الاحتياطات الوقائية ضد تعرضها لخطر ما . ففي حالة الحروب يجب الحرص على هذه الوثائق وحمايتها من التعرض للدمار والضياع، وذلك بترتيب الوثائق في مجموعات، وتسجيلها في قائمة من نسختين لبيان محتويات كل مجموعة، ويتم وضع نسخة مع الموظف المختص، وتوضع نسخة أخرى في صندوق يفضل أن يكون معدنياً وموجوداً في مكان غير أماكن العمل مع ضرورة وضع مواد كيماوية في الصناديق لامتصاص الرطوبة وقتل الحشرات والفطريات التي تضر بالأوراق خلال فترة حفظها.

4) الأمن من التقادم الطبيعي وسوء الحفظ:

الحفظ "هو عملية ترتيب وتخزين الوثائق بنوعياتها المتعددة بنظام يضمن سلامتها ويمكن الوصول إليها بسهولة إذا ما أريد الرجوع إليها".

وعليه إن إساءة حفظ الوثائق يؤدي إلى تلفها وتعرض سلامتها إلى الضرر. لذا لابد من الحرص على توفير إمكانيات مناسبة لحفظ هذه الوثائق من توفير أماكن ذات تهوية جيدة، ومزودة بأثاث معدني للحفظ السليم، وذلك كله يعد ضرورة ملحة لحماية هذه الوثائق وفي الوقت نفسه يشكل ذلك مشكلة توعرق القائمين على أعمال الأرشيف.

أما حول التقادم الطبيعي للأوراق المخزنة فتعود أسبابه إلى ما يلي:

أ-**الضوء**، ويعتبر الضوء الطبيعي كضوء الشمس والضوء الصناعي من مسببات تلف الأوراق، إذ يؤثران على لونها وعلى قوة تماسكها .

ب-**الرطوبة**، وتعد من أخطر الأمراض التي تصيب الأوراق، وبخاصة في البلاد ذات الأجواء الباردة.

ج-**الأتربة والغازات الضارة**، وهي عوامل تلحق الضرر بالأوراق، وبمعدات حفظ الوثائق المعدنية.

د- **ارتفاع الحرارة**، إذ يؤثر ارتفاعها عن المعدل المطلوب على الورق، فيتغير لونه إلى الأصفر ويصبح هشاً قابلاً للكسر.

أمن الوثائق والميكروفيلم (حمودة،د.ت،(37-44)).

كثيراً ما تكون الوثائق الهامة مثل العقود، والمعاهدات، ونتائج الامتحانات فريسة مستهدفة من عدد من الأفراد؛ فقد تتعرض للسرقة، أو للضياع، أو التلف، أو التزوير، مما يعرض حقوق الأفراد، وحقوق الصالح العام إلى الضياع.

ولحماية هذه الوثائق المهمة، وتحقيق أمنية لها، وتقليلاً لاحتمالات التزوير، والعبث، ظهر الميكروفيلم باعتباره وسيلة أمن وحماية للوثائق، ليس فقط من التزوير، وإنما أيضاً من التلف الناتج عن كثرة التداول والاطلاع.

وعرف الميكروفيلم على انه" مساحة فيلمية ذات خصائص معينة تسجل عليها كمية من المعلومات تقرأ، أو تطبع على ورق خاص، وأفلام خاصة بواسطة أجهزة قراءة، وطباعة معينة" .

بعض الفوائد المتحققة من استخدام الميكروفيلم:

1-توفير (98%) من المساحة اللازمة لحفظ الوثائق الأصلية.

2-توفير الأمان للوثائق.

3-اختصار الوقت المطلوب للوصول إلى الوثائق المصورة إلى ثوانٍ معدودات.

4-تحقيق السرية للمعلومات المحفوظة على الميكروفيلم لأنه لا يمكن قراءتها بالعين المجردة.

5-توفير سلامة وموثوقية للمعلومات المحفوظة، وذلك بالتخلص من الأخطاء التي تحدث عند نقل الوثيقة بالكتابة على الآلة الكاتبة، أو باليد.

وعليه جاء الميكروفيلم باعتباره وسيلة مساندة في توفير حماية وأمان وسلامة المعلومات من التعرض لسرقة، أو لخطر، أو تهديد سواء كان خارجياً أو داخلياً مقصوداً أو غير مقصود.

ثانياً:دور القانون في أمنية العمل الحكومي

يلاحظ عند الرجوع إلى الجريدة الرسمية وتحديداً إلى قانون حماية أسرار ووثائق الدولة رقم (50) لسنة(1971)، مدى حرص واهتمام المشرع بالحفاظ على أمن المعلومات وسلامتها والأسرار خاصة المتعلقة بالدولة لتحقيق أمن قومي شامل، إذ تناول هذا القانون عدداً من المواد كان محتواها يركز على تحديد نوع المعلومات المدرجة وصنف الوثائق حسب درجة السرية إلى (سري للغاية، وسري، ومحدود السرية) وحدد المعلومات المدرجة تحت كل صنف ودرجة من السرية. كما حدد إجراءات التعامل مع المعلومات وطرق حفظها حسب درجة سريتها، وبين نطاق مهمات الموظف المسؤول عن المعلومات السرية، وأكد على استمرار مسؤولية هذا الموظف عن المعلومات وسريتها حتى بعد انتهاء الخدمة أو النقل ، كما تم تحديد عقوبة سرقة الوثائق أو إفشاء أسرارها سواء كان لصالح جهات في البلد نفسه أو لمنفعة دولة أجنبية، وبيان مقدار العقوبة في كلتا الحالتين مع شدتها في حال اقترفت الجناية لمنفعة دولة أجنبية، إذ حددت هذه العقوبة بالأشغال الشاقة المؤبدة، وبالإعدام إذا كانت هذه الدولة الأجنبية عدواً ، أما إذا كانت سرقة المعلومات أو إفشاؤها لمصالح جهات في البلد نفسه؛ فتكون العقوبة بالأشغال الشاقة لمدة لا تقل عن عشر سنوات (الجريدة الرسمية، 1971،(1164-1166)).

يلاحظ من خلال العقوبات السابقة أنها عقوبات صارمة وجادة مما يدل على عدم تساهل المشرع الأردني في هذا الموضوع، ويشير إلى أهمية هذه المعلومات والأسرار، ومقدار الحرص على حمايتها، وتوفير السلامة والأمان لها.

ثالثاً:العمل الحكومي الإلكتروني والأمنية:

1-الحكومة الإلكترونية :(المفهوم والفلسفة، والركـائز، والمحتـوى، والفوائـد المتطلبات، والمراحل، والصعوبات).

إن تزايد عدد الأفراد في المجتمعات واحتياجاتهم، وارتفاع مستوى وعيهم لما يقدم لهم من خدمات ولحقوقهم وطلبهم الحصول على الخدمات ذات الجودة العاليـة وعدم مناسبة الأساليب اليدوية لإنجاز معاملاتهم في ضوء التطورات المتسارعة في عصر المعلوماتية. وتقادم الأساليب اليدوية، واتسامها بالبطء، والتعقيد، واستهلاكها للوقت، والجهد، والمال، كلها عوامل تجعل الحكومة الإلكترونية هي المسلك المؤدي إلى سرعة إنجاز المعاملات، وسهولة الحصول على الخدمات ذات الجودة العاليـة، وتحقيق العدالة والمساواة بين المواطنين من خلال حق الجميع في الحصول علـى الخدمة والمعلومة، فالحكومة الإلكترونية في عصرنا الحاضر هي الأمل الذي تستند إليه الدول وتتعلق به لحل المشاكل السابقة، والتخفيف من حدتها.

ومع بزوغ فجر المعلوماتية وانتشار الحاسوب والتجارة الإلكترونية، أصبحت الحكومة الإلكترونية ضرورة وحاجة ملحة لا بد من تبنيها والبدء بتنفيذها بأسـرع وقت مع ضرورة القيام بإجراء التعديلات اللازمة كمتطلبات لتطبيقها ومسـتلزمات ضرورية لتحقيقها حتى نواكب ركب التطور الذي تشهده الدول المتقدمة في العالم.

واستجابة لذلك "وفي وقت متقارب، أطلقت ثلاث دول عربيـة هـي الأردن، ومصر، والإمارات مشاريع بناء الحكومة الإلكترونية، وباشـرت حكـومتي قطـر والسعودية بتنفيذ مشاريع شبيهه،وهي فكره أثارها ونادى بها نائب الرئيس الأمريكي السابق (آل جور)،ضمن تصور لديه لربط المواطن بمختلـف أجهـزة الحكومـة للحصول على الخدمات الحكومية بأنواعها بشكل آلي ومؤتمت، إضافة إلى إنجـاز الحكومة ذاتها مختلف أنشطتها باعتمادها شبكات الاتصال والمعلومات لخفض الكلف وتحسين الأداء وسرعة الإنجاز وفعالية التنفيذ".(عرب، 2001، 445)

ويعتبر الإنترنت هو الوسيلة التي يتم من خلالها تحقيق مشروع مثل التجـارة الإلكترونية والحكومة الإلكترونية، وخير شاهد على أهمية شبكة الإنترنـت وعظـم دورها هو سرعة انتشارها مقارنة مع الاختراعات الأخرى التي كان لها دور فـي

حياة الإنسان، إذ استغرق الإنترنت (6) سنوات بين ظهوره وابتكار الـ Web وانتشار استخدام الإنترنت في معظم أرجاء العالم، وهي مدة قصيرة مقارنة مع اختراعات أخرى مثل الكهرباء التي استغرقت (46) سنة ، والهاتف (35) سنة ، والحاسوب الشخصي (16) سنة، والهاتف الخلوي (13) سنة؛ فهذا هو خير شاهد على أهمية الإنترنت، وعلى تجاوب الدول، واستشعارها بأهمية الحاسوب بوصفه متطلباً من متطلبات عصر المعلوماتية.(الكيالي،2000،11).

مفهوم الحكومة الإلكترونية:(LANVIN, 2002,1)

من المزايا الإيجابية للثورة الرقمية قدرتها على تعزيز الديمقراطية ودفع الحكومات إلى الاستجابة بصورة أكبر لمتطلبات مواطنيها، ويشير مفهوم الحكومة الإلكترونية إلى استخدام تقنيات المعلومات والاتصالات (ICT): Information Communication Technology بهدف تغيير أداء الحكومة من خلال جعلها اكثر فعالية ومسؤولة، وتشتمل الحكومة الإلكترونية على التالي:

1. تأمين وصول أكثر إلى المعلومات الحكومية.
2. تعزيز المشاركة الشعبية من خلال تمكين الجماهير من التفاعل مع موظفي الحكومة.
3. جعل الحكومة عرضة للمساءلة بصورة اكبر من خلال تميز أنشطتها بالشفافية مما يحد من احتمال الفساد.
4. تأمين الفرص التنموية، وبالأخص لسكان الأرياف والأقل حظاً أو اقل خدمة.

والحكومة الإلكترونية ليست بالأداة المقتصرة على الدول الغنية فحسب، إذ تشير الحقيقة إلى أن بعض الاستخدامات الأكثر إبداعية لشبكة الإنترنت تظهر في البلدان النامية حيث تستخدم تكنولوجيا المعلومات والاتصالات لتحديث الحكومة وربطها عن كثب وبصورة أكبر مع المواطنين الذين يفترض خدمتهم.

والحكومة الإلكترونية ليست دواء من كل داء، فبالرغم من قدرتها على تسهيل عملية التغيير وخلق عمليات إدارية جديدة وأكثر فعالية، إلا أنها لن تحل جميع المشكلات المرتبطة بالفساد وعدم الكفاءة، كما أنها لن تتغلب على جميع

عوائق المشاركة الجماهيرية. لكنها تعمل على تحسين ظروف حياة الناس في الدول النامية من خلال تحسين وتسهيل الوصول إلى المعلومات المفيدة لهؤلاء الناس في حياتهم اليومية مع سعي الحكومة الإلكترونية إلى تقديم الخدمات وطرح فرص المشاركة الجديدة في العملية السياسية.

ورغم حداثة المصطلح نوعاً ما، إلا أن تعريفاتها كثيرة ومتنوعة، إذ عرفها الزعبي على أنها"مقدرة الحكومة على تحسين الخدمات التي تقدمها إلى المواطنين من خلال استخدام التكنولوجيا". (الزعبي، 2000،12).

كما عرفت بأنها تعني للمواطن" الانتقال من الوقوف في الطابور من اجل الحصول على الخدمة الحكومية إلى تحصيل الخدمة مباشرة عبر شبكة الإنترنت وفي الوقت الذي يناسبه".(الكيالي،2000،11).

وعرفت أيضاً بأنها" البيئة التي تتحقق فيها خدمات المواطنين واستعلاماتهم وتتحقق فيها الأنشطة الحكومية للدائرة المعنية في دوائر الحكومة بذاتها أو فيما بين الدوائر المختلفة باستخدام شبكات المعلومات والاتصال عن بعد".(عرب،2001،447).

فلسفة الحكومة الإلكترونية

لابد من العلم بأن الحكومة الإلكترونية تتناول قضية التحول، وأن التكنولوجيا هي الأداة المستخدمة لذلك التحول، والحكومة الإلكترونية ترتبط بعملية التحول التي تسعى لمساعدة المواطنين، والحكومات، والأعمال التجارية على إيجاد فرص جديدة في الاقتصاد المعلوماتي العالمي.

كما ينبغي أن تستغل الحكومة الإلكترونية لإعادة النظر في دور الحكومة، وأن تستخدم باعتبارها أداة نحو المزيد من التنمية الاقتصادية والحكم الجيد. والحكومة الإلكترونية ليست بالأمر البسيط أو غير المكلف. فقبل توفير الوقت والموارد اللازمة في عملية التطبيق الناجح يتحتم معرفة أسباب تبني هذه الفكرة، التي لا تتحقق بمجرد إصدار التشريعات والأوامر الصادرة عن القيادات السياسية بتبنيها، إنما تتطلب العملية تغيير الكيفية التي يعتمدها الموظفون في طريقة تفكيرهم، سلوكهم، ورؤيتهم لأعمالهم، والكيفية التي يتبادلون من خلالها المعلومات كما

تتطلب إعادة هندسة المنظمات الحكومية والتجارية، وسرعة في التجاوب مع التغيرات الداخلية والخارجية المحيطة بالمنظمات الحكومية والتجارية في مجال التكنولوجيا، فإدخال الحواسيب لا يعني الإصلاح أو حدوث التغيير، إنما يجب التركيز على إدخال تكنولوجيا المعلومات والاتصالات، وبناء مجتمع المعلومات الذي يتم فيه تمكين حياة المواطنين وإثرائها من خلال الوصول إلى المعلومات والفرص الاجتماعية، والاقتصادية، والسياسية التي توفرها هذه المعلومات بشكل سريع وبفرصة متساوية لكل مواطن.

وتعد عملية اختيار مشروعات الحكومة الإلكترونية، وبالأخص المشروعات التجريبية الأولى منها، من أكثر الخطوات حساسية وخطورة، إذ إن المشروع الأول الناجح هو نقطة البداية بالنسبة لجميع الجهود المستقبلية، كما قد تغدو قضية النجاح الصغيرة مثالاً بارزاً يسعى الآخرون إلى محاكاته والاسترشاد به .

ولا بد قبل اختيار مشروع ليكون بداية نقطة الانطلاق من عمل تشخيص للأوضاع الراهنة، وجمع معلومات حول أكثر المشروعات أهمية للمواطنين، وأكثرها احتكاكاً معهم، وتحديد الوضع الحالي لتكنولوجيا المعلومات والاتصالات، وتحديد مستوى الأوضاع الاقتصادية للبلد، والمخصصات المرصودة لمشروع الحكومة الإلكترونية.

وتمثل هذه المعلومات التي تم جمعها قاعدة يتم على أساسها قياس حجم الإمكانيات المتاحة، وتوقع حجم التقدم المحتمل للمشروع. كما أن الاستفادة من التجارب الناجحة بالدول السابقة في التطبيق من أهم الأمور التي يجب أن لا تغفل عنها. فلا بد من زيارة هذه الحكومات والحديث مع القائمين على المشروع حول التجربة، واخذ المشورة منهم مع أهمية أن تخضع عملية التكييف للمواءمة مع الظروف المحلية الخاصة بالدولة.

وللمشاركة الجماهيرية في عملية التحول نحو الحكومة الإلكترونية بالغ الأثر والأهمية؛ فعندما يتطرق الحديث إلى موضوع الحكومة الإلكترونية والمشاركة الجماهيرية، فإن جميع البلدان تعد دولاً نامية حتى اكثر الدول تقدماً تسعى إلى تعلم تشجيع المشاركة الجماهيرية، وتنظيمها، وادارتها.

فقضية المشاركة الجماهيرية تعد عنصراً هاماً في العديد من مراحل عمل الحكومة الإلكترونية، فالحكومة الإلكترونية لا تساوي الأتمتة، إنما تساوي المشاركة. وطرق مشاركة الجمهور في الحكومة الإلكترونية متعددة أبرزها.

أ-التعليق على خطط الحكومة الإلكترونية ذاتها.

ب-استرجاع المعلومات مثل الوصول إلى المعلومات من خلال المواقع الحكومية، أو تقديم المعلومات من خلال الاستطلاعات الشعبية والبريد الإلكتروني.

ج-المشاركة في الحوارات سواء ما كان منها بين الجماهير والحكومة أو بين المواطنين أنفسهم.

إذاً، لابد من تضمين جميع أنواع المشاركة الجماهيرية في خطط الحكومة الإلكترونية، وطرح صور متعددة من المشاركة، ضماناً للاستماع لجميع الأصوات والآراء مع الحرص على توفير فرص مشاركة الجماهير بالطرق التي تعنيهم، ولابد من أن يتلمس المواطنون عوائد هذه المشاركة، وأن تؤخذ آراؤهم بالاعتبار من خلال حصول التعديلات، وحل المشكلات التي يواجهونها. كما يعد التعاون بين الحكومات والقطاع الخاص والجماهير من أهم عناصر الجاهزية. ولا بد من أن يبنى التعامل بين قاده مشروع الحكومة الإلكترونية على أساس التعاون والاتصال المستمر، وأن يقودوا دفة جهد الحكومة الإلكترونية بشكل مرن وأكثر بساطة وشفافية من خلال استبدال مفهوم الأمر والرقابة بمفهوم التفاعل والمشاركة. ونظراً لأهمية دور المواطنين، فإنهم يعتبرون بمنزلة خبراء في الحكومة الإلكترونية، وبخاصة أن الهدف من الحكومة الإلكترونية، في نهاية المطاف، هو خدمة هؤلاء المواطنين. وعليه فإن تقييم احتياجاتهم، وتثمين مشاركتهم يعتبران قضية ذات أهمية خاصة في المشروعات المتضمنة على خدمة الجمهور بشكل مباشر. وعلى الحكومة الإلكترونية عند تقديم خدماتها للمواطنين الاسترشاد بالمشاركة الكاملة لهم، لأنه إذا تمت المباشرة قبل أخذ آرائهم وردود فعلهم، فقد يكون المشروع عرضة لمخاطرة كبيرة. لذا لا بد من تسهيل مشاركة المواطنين، وأن لا ينظر لهذه المشاركة على أنها هم ثقيل، فالتكنولوجيا الحديثة تؤدي دوراً تسهيلياً، إذ توفر قنوات اتصال سريعة وغير مكلفة. (PACIFIC COUNCIL, 2002 ,7 -24)

ركائز الحكومة الإلكترونية

يستند مفهوم الحكومة الإلكترونية إلى ركائز أربع، إذ توضح هذه الركائز مفهوم الحكومة الإلكترونية وفكرتها:-

1-تجميع وتركيز جميع الأنشطة والخدمات المعلوماتية والتفاعلية والتبادلية في مكان واحد؛ وهو موقع الحكومة الرسمي على شبكة الإنترنت في نشاط أشبه ما يكون بفكرة مجتمعات الدوائر الحكومية، حتى يتسنى للمواطن الاتصال والاستفادة من أكثر من دائرة أو مؤسسة في الوقت ذاته والمكان نفسه.

2-تحقيق حالة اتصال دائم ومستمر بين الجمهور والدوائر والمؤسسات الحكومية (24 ساعة في اليوم و 7 أيام في الأسبوع و 365 يوماً في السنة)مع القدرة على تأمين جميع الاحتياجات الاستعلامية والخدمية للمواطن بشكل مستمر دون انقطاع.

3-تحقيق سرعة وفعالية وكفاءة في الربط والتنسيق والأداء والإنجاز بين دوائر ومؤسسات الحكومية مع بعضها البعض ولكل منها على حدة.

4-تحقيق وفرة في الإنفاق في العناصر كافة بما فيها تحقيق عوائد افضل واكثر من الأنشطة الحكومية ذات الطابع والمحتوى التجاري. (عرب،2001،446)

محتوى الحكومة الإلكترونية

تتكون الحكومة الإلكترونية من مجموعة من المحتويات الأساسية تتصف بالتنوع؛ فهي تنحصر بين محتويات خدمية، ومعلوماتية، واتصالية:

أ-محتوى معلوماتي: يغطي كافة الاستعلامات تجاه الجمهور أو بين مؤسسات ودوائر الدولة مع بعضها البعض، أو بين هذه المؤسسات والدوائر من جهة، وبين مؤسسات الأعمال منّ جهة أخرى.

ب-محتوى خدمي: يتيح تقديم جميع الخدمات الحياتية، وخدمات الأعمال للجميع بشكل متساوٍ، وبصورة مباشرة.

ج-محتوى اتصالي: (وهو ما يسمى خلق المجتمعات) يتيح ربط إنسان الدولة وأجهزة الدولة في كل وقت ومن أي مكان بوسيلة اتصال وتفاعل سهلة. (عرب، 2001،448).

فوائد الحكومة الإلكترونية

يتوقع أن تعم فوائد الحكومة الإلكترونية جميع الأطراف التي يضمها المجتمع على اختلاف أدوارهم وأعمارهم ومستوياتهم، وأهم الأطراف المستفيدة من الحكومة الإلكترونية، وأبرز فوائدها :

أ-**المواطن أو الجمهور**، يتوقع المواطن أو الجمهور أن تحقق له الحكومة الإلكترونية فوائد متنوعة تشتمل على توفير الخدمة بشكل أفضل وأسرع وفي وقت أقل وجودة أعلى مع إمكانية الحصول على هذه الخدمة بشكل مستمر في كل الأوقات، وكذلك السعي إلى تخفيف العبء عن كاهل هذا المواطن من ناحية الجهد المبذول في الحصول على الخدمة، وتوفير المال والوقت المستغرق في إنجاز هذه الخدمة أو الحصول على المعلومة . وكذلك السعي نحو تحقيق قدر من الشفافية من خلال الإتاحة الكاملة والمتساوية للوصول لمعظم المعلومات المرتبطة بالقرارات والإجراءات الحكومية ذات العلاقة بالخدمات، وتحقيق الشعور بالمساواة والعدالة من خلال تساوي الجميع في الحق بالحصول على المعلومات والاستفادة من الخدمات.

ب-**المنظمات الخاصة**، ونظراً لما للمنظمات الخاصة من دور لا يمكن إنكاره في خدمة المواطنين ومساعدة الدولة في تقديم جزء من الخدمات والتفرد في بعضها أحياناً ، فإن العلاقة القائمة على التعاون بين القطاع العام والخاص تحتم استفادة كلا الطرفين من بعضهما البعض وعند قيام الدولة بالتحول نحو الحكومة الإلكترونية، فإن من شأن ذلك التأثير على القطاع الخاص. ومن أهم الفوائد التي يجنيها القطاع الخاص من جراء التحول نحو الحكومة الإلكترونية أنها تتيح أداء العمليات التجارية بين المنظمات الخاصة والعملاء وبينها وبين المنظمات الحكومية وبين المنظمات الخاصة مع بعضها البعض من خلال استخدام تكنولوجيا المعلومات والاتصالات. كما تساعد في تخطي الحدود الزمنية والمكانية التي تقيد حركة التعاملات التجارية، وتمكين المنظمات الخاصة من الاستجابة السريعة لطلبات السوق، وزيادة القدرة التنافسية، وتخفيض التكاليف، ورفع مرونة إدارة الأعمال وتقديم الخدمات .

ج-**الحكومة:** الطرف الثالث المستفيد من تطبيق الحكومة الإلكترونية، إذ يعود توجه الحكومة نحو التحول إلى العمل الإلكتروني بفوائد عظيمة تتجلى في تغيير انطباعات المواطنين بشأن النوعية الروتينية للخدمات العامة التي تقدمها لهم، والمساعد في إعادة ثقة المواطنين ومصداقيتهم بالحكومة، والمساهمة في تقليل نسبة التعقيد، وتبسيط إجراءات العمل بين الحكومة والمواطنين، واختصار التكاليف والوقت المستغرق في إنجاز المعاملات، والحصول على الخدمات مع ارتفاع في جودة الخدمة المقدمة إلكترونياً، وزيادة الشفافية في الأعمال الحكومية من خلال الانفتاح في الاتصال بين المواطن والدوائر، والمؤسسات الحكومية بصورة تسهل التعامل مع الجهاز الإداري، مع إمكانية تقليل نسبة الأخطار الإجرائية ومنع الاجتهاد الشخصي للموظفين الحكوميين في تفسير القوانين والتعليمات كما تسهل على الموظفين الحكوميين متابعة إجراءات العمل. (جبر ، 2002،(188-192)).

متطلبات بناء الحكومة الإلكترونية

وأهم هذه المتطلبات وأكثرها إلحاحاً :-

أ-حل المشكلات القائمة في الواقع الحقيقي قبل التحول إلى البيئة الإلكترونية، وهذا يتطلب من الحكومات توفير المعلومات اللازمة لمواطنيها عبر الإنترنت مع الحرص على توفير سياسة واضحة يتم بموجبها تحديد جميع الوثائق والمعلومات والنماذج الحكومية بشكل مباشر، بحيث تكون الحكومة مكلفة بنشر كل المعلومات الجديدة والوثائق الحكومية الجديدة على الإنترنت فور صدورها. ومن أهم المشاكل التي نلحظها في واقع العمل عبر البريد الإلكتروني مشكلة التوثيق، إذ لا يوجد نظام توثيق فاعل يضع جميع وثائق العمل الحكومي في موضعها الصحيح وفي الوقت المطلوب لذلك يجب العمل على حل هذه المشكلة ومثيلاتها في واقع العمل الحكومي غير الإلكتروني قبل الانتقال إلى العمل الحكومي الإلكتروني.

ب-حل مشكلات قانونية التبادلات التجارية، وتوفير وسائلها التقنية والتنظيمية، وذلك من منطلق أنه سيتم وضع جميع المبادلات التي تتعامل بالنقود عند التحول إلى العمل الإلكتروني عبر الإنترنت مثل، إمكانية دفع الفواتير والرسوم الحكومية

المختلفة مباشرة وعبر الإنترنت، وجعل هذه العملية بينية، أي تتضمن كل من يقوم بأداء التعاملات التجارية في المؤسسات الحكومية.

ج-توفير البنى والاستراتيجيات المناسبة التي يكفل من خلالها بناء المجتمعات، إذ يتطلب بناء هذه المجتمعات إنشاء وسيط تفاعلي على الإنترنت يضمن تفعيل التواصل بين المؤسسات الحكومية مع بعضها البعض، وبين المؤسسات الحكومية والمواطنين. وبينها وبين مزوديها، بحيث تمكن من توفير معلومات بشكل مباشر حول أي عملية تجارية تم إنجازها في وقت سابق بالإضافة إلى استخدام مؤتمرات الفيديو باعتبارها وسيلة تسهل الاتصال بين الموظف الحكومي مقدم الخدمة والمواطن متلقي لهذه الخدمة . (عرب ،2001،(451-452)).

مراحل تطبيق الحكومة الإلكترونية والإجراءات التي تتطلبها كل مرحلة.

إن مشروعاً مهماً على صلة بكل شرائح المجتمع هو بحاجة إلى عناية وجهد كبيرين وتفكير عميق قبل الإقبال عليه وتنفيذه.

وليس من الحكمة ولا من الصواب أن يتم تنفيذ مشروع الحكومة الإلكترونية دفعة واحدة، بل من الأسلم أن يتم تنفيذها بشكل مرحلي من ناحية التطبيق، وكذلك من حيث المؤسسات والمجالات التي سوف يتم التطبيق فيها، إذ يفضل اختيار المؤسسات العامة ذات التماس اليومي مع المواطنين كمشروع ريادي تطبيقي للحكومة الإلكترونية، وان يتم التركيز على مجال محدود. ويسهم التطبيق المرحلي في ضمان فرص أكبر للنجاح، وتحقيق إنجاز أسرع، وتلمس المشاكل ومعالجتها بكفاءة أعلى، ويمنع تكرار الأخطاء، ويبني الخبرة الكامنة والمتراكمة لدى الجهاز الحكومي والكفاءات العاملة فيه، كما يشجع نجاح هذا القطاع التجريبي قطاعات ومؤسسات أخرى على تبني الفكرة وتعميم التجربة لتشمل المؤسسات الحكومية كافة.(عوجان،2000،(10-11))

وهناك أربع مراحل متسلسلة ومهمة يتطلبها تطبيق الحكومة الإلكترونية، ويتبعها جملة من الإجراءات بوصفها مستلزمات لتطبيق هذه المراحل.(القطامين وعواد،2002،(4-5))

أولاً :عرض المعلومات من خلال قيام الحكومة ممثلة بوزاراتها ومؤسساتها بنشر المعلومات الكاملة عنها على الإنترنت في مواقع إلكترونية، وتحميل النماذج والاستمارات الحكومية على هذه المواقع، وهي مرحلة اتصال أحادية الجانب.

وأبرز الإجراءات الحكومية التي تتطلبها هذه المرحلة:-

1-تطوير البنية التحتية التي تشتمل على البنى الأساسية لنظم الاتصالات مما يمكن من زيادة عدد الهواتف الثابتة والمحمولة المستخدمة في المجتمع.

2-تشجيع الأفراد والمؤسسات على استخدام الهواتف بشكل أكبر من خلال خفض أسعار الاتصالات الهاتفية.

3-العمل على دعم أسعار أجهزة الحاسوب حتى تشجع أسعارها جميع فئات المجتمع على اقتناء هذه الأجهزة.

4-اتخاذ التدابير والإجراءات المساعدة على زيادة المنافسة بين الشركات التي تقدم خدمات الإنترنت مما ينعكس بالطبع على تخفيض أسعار اشتراكات الإنترنت.

5-تبني الحكومة استراتيجية وطنية تهدف إلى زيادة إمكانية ربط دخول الأفراد والمؤسسات إلى شبكة الإنترنت، وذلك من خلال إتاحة الوصول إلى الإنترنت بوساطة المؤسسات الحكومية والخاصة، والمكتبات العامة، والمراكز الثقافية، والجامعات، والمدارس.

ثانياً:تطوير نظم الاتصالات المتبادلة حتى تصبح المواقع الإلكترونية وسيلة اتصال ثنائية تسمح للأفراد والمؤسسات بالاستفسار عن المعلومات وملئ الاستمارات والنماذج التي تتطلبها عملية تقديم خدمات الدولة إلى مواطنيها إلكترونيا بالإضافة إلى إمكانية تلقي الإجابات عن الاستفسارات من قبل الدوائر والمؤسسات المعنية.

وأبرز الإجراءات التي تتطلبها هذه المرحلة:-

1-توفير المعلومات والمعطيات واعتبارها ملكية عامة تحميها تشريعات وقوانين تتناسب مع تطورات الحياة في عصر المعلوماتية.

2–قيام الحكومة بحملة شاملة لإدخال الإنترنت إلى جميع المدارس والمعاهد والجامعات من أجل ترسيخ ثقافة تكنولوجيا المعلومات لدى الأجيال.

3–تبني الحكومة لاستراتيجيات وطنية شاملة لتدريب العاملين كافة في قطاع التعليم والعاملين في مجال تكنولوجيا المعلومات بشكل خاص مع الحرص على رصد مخصصات مناسبة من ميزانية الدولة ومؤسسات القطاع الخاص لتمويل هذه الدورات التدريبية.

ثالثاً: تبادل المنفعة والقيمة، إذ ينتج عن تطبيق الحكومة الإلكترونية منفعة متبادلة بين الحكومة ومواطنيها، حيث توفر المواقع الإلكترونية تبادلاً أفضل للمنفعة بين الحكومة ومواطنيها، ويكون الاتصال أسهل؛ فالمواطن يتمكن مثلاً من استخراج شهادة ولادة أو معاملة ترخيص بسرعة فائقة، وكلفة اقل، ومجهود بسيط، فالحكومة تخدم مواطنيها بمستوى عالٍ من الفاعلية وبأقل جهد وتكلفة.

أبرز الإجراءات التي تتطلبها هذه المرحلة.

1. التحول بشكل جذري وجدي من العمل التقليدي اليدوي إلى العمل الإلكتروني، وهذا التحول يحتاج إلى تغيير جذري في الإجراءات والهياكل والتشريعات.
2. تشجيع قطاع المصارف والمال على تطوير أساليبها وتبني استراتيجيات ووضع نظم تضمن المحافظة على سرية التعاملات المالية وسلامتها.

رابعاً : التكامل بين الخدمات الحكومية، وهذا يحتم على الحكومة تطوير وزيادة فاعلية نظم نقل المعلومات وشبكات توزيعها أفقياً وعمودياً، بحيث يصبح الاهتمام والعناية بالحاجات الفعلية والأنشطة بدلاً من التركيز على الفئات والإدارات المحددة.

وأبرز الإجراءات التي تتطلبها هذه المرحلة:-

1. تركيز الدولة واهتمامها نحو إنشاء أنظمة فعالة ضماناً لسرية المعلومات الخاصة بالأفراد والمؤسسات التي بدورها تضمن بناء الثقة لدى مستخدمي المواقع الإلكترونية.

2. سن القوانين والتشريعات الرادعة للمتطاولين والمتطفلين علـى أمنيـة الحكومـة الإلكترونية.

بعض الصعوبات التي تواجه بناء الحكومة الإلكترونية

1-المحافظة على الخصوصية: إذ تشير الدراسات إلى أن (34%) من المتعاملين مع الإنترنت ينتابهم شعور بأن الإنترنت يهدد الخصوصية، الأمر الـذي يسـتدعي وضـع إجراءات وتعليمات لضبط وتحديد استخدام المعلومات الواردة عن طريق الإنترنت، كمـا يجب وضع التشريعات لضمان المحافظة على خصوصية الملفات العامة الحكومية.

2-التخويل: إذ يشتكي التجار من أن نصف عمليات الشراء التـي تـتم بوسـاطة بطاقات الائتمان هي مزورة. لذلك لا بد من اتخاذ الإجراءات الوقائية التالية:-

أ-التأكد من هوية المواطن .

ب-التأكد من التوقيع الإلكتروني .

ج-التأكد من جاهزية البنية التحتية والاستعداد لإجراءات الصيانة لهذا النوع من المعاملات.

3-تبادل المعلومات، تكون المعلومات عرضة للاعتداء عليها أثناء تبادلها، وعليـه يجب الاهتمام بالمعلومات التي يتم استلامها من المواطنين، والحرص على استلامها ضمن صيغ محددة، ووضعها في النظام، والمحافظة عليها من الضياع.

4-عدم توافر عدد كافٍ من المواقع الجديدة على الإنترنت، وعدم وجـود تـرويج ودعاية مناسبة وكافية. من ناحية أخرى عدم توافر أدوات مناسبة تمكن المواطن من الوصول إلى الموقع أو الجزء المطلوب من المعلومات المتـوافرة فـي الموقـع و صعوبة تحديث معلومات الموقع آنياً، إضافة للصعوبات المتعلقة بتقديم الدعم الكافي والخدمات لمستخدمي النظام. (الزعبي، 2000،(13-14))

متطلبات نجاح مشروع الحكومة الإلكترونية :

حتى نضمن أن تتكلل هذه التجربة وهذا المشروع بنجاح، لا بد من الحرص علـى عدد من المتطلبات التي قد تأخذ شكلاً إلزامياً لتصبح شروطاً لنجاح الحكومة الإلكترونية. ومن أهم هذه المتطلبات :

1-التطبيق المرحلي لمشروع الحكومة الإلكترونية، وتطبيقه على مستوى بعض المجالات والمؤسسات، وعند نجاح المشروع التجريبي يتم تعميم التجربة.

2-الاهتمام بالقضايا الحساسة والأساسية التي لا بد من معالجتها في النظم المكونة للحكومة الإلكترونية مثل: السرعة؛ وأمنية المعلومات؛ والمحافظة على السرية والخصوصية؛ والدقة؛ وامكانية التعامل؛ والاستخدام الميسر لهذه التكنولوجيا.

3-إعادة هندسة البنية التحتية، والهياكل، والعمليات، والإجراءات، بما يتناسب مع التكنولوجيا الحديثة، بحيث لا يقتصر التغيير والتعديل على الإجراءات، وتسلسل إنجاز المعاملات، وإدخال الأجهزة المطورة والمعدات الحديثة والبرمجيات اللازمة لتشغيلها بل ويشتمل أيضا على تغيرات في الهياكل والبنى التنظيمية وتعديلات على الوصف الوظيفي للوظائف وإعادة النظر في توزيع المهام على الموظفين، وتغيير طبيعة العمل نفسها لتصبح أكثر فاعلية وإنتاجية وأقل جهداً، أي أفضل جودة.

4-تنمية الموارد البشرية وتطويرها، إذ لا بد من تأهيل الموظف من الناحية الفنية ليصبح قادراً على التعامل مع التكنولوجيا الحديثة، وكذلك بناء ثقافة اجتماعية وتنظيمية للمواطن والموظف تجاه تكنولوجيا المعلومات، والحرص على تبني سياسات تدريبية دورية للعاملين حتى يواكبوا كل التطورات، وكل ما هو حديث على ساحة تكنولوجيا المعلومات.

5-بناء ثقة لدى المواطن تجاه مشروع الحكومة الإلكترونية، وذلك من خلال نشر توعية عامة عن الحكومة الإلكترونية، وتلمس المواطن لفوائد الحكومة الإلكترونية من خلال الحصول على فوائد ملموسة متمثلة بإتمام المعاملات الخاصة به بدقة وسرعة، ولا تكفي التوعية العامة وتلمس الفوائد لنجاح الحكومة الإلكترونية بل لا بد من شعور المواطن بالأمان تجاه ما يخصه من معلومات على أنها ليست مشاعاً بل محاطة بإجراءات الأمن والحماية المناسبة للخصوصية.

6-إيجاد مناخ قانوني يستجيب لمتطلبات الحكومة الإلكترونية لضمان المحافظة على السرية والخصوصية والأمن والحماية للمعلومات، وذلك بسن القوانين الجديدة وتعديل التشريعات والقوانين والأنظمة التي تنظم أعمال المؤسسات الحكومية.

7-توفير الدعم السياسي والمالي لمشروع الحكومة الإلكترونية من خلال تبني الفكرة ودعمها من جهات سياسية مهمة في الدولة، وكذلك رصد ميزانية مستقلة ومستمرة لتمويل مشروع الحكومة الإلكترونية . (جبر،2002،(200-201)) و(عوجان،2000،(10-11))

2-أمنية الحكومة الإلكترونية وسريتها:

إن نجاح مشروع كبير، مثل الحكومة الإلكترونية، يحتاج إلى دعم واسع من جميع الأطراف العاملة عليه والجهات المستفيدة منها، وليس بالامكان كسب دعم هذه الأطراف والجهات والحصول على ثقتها، إلا من خلال تمايز هذا الأسلوب (العمل الإلكتروني) عن الأسلوب السابق له (العمل التقليدي، اليدوي). وتتحقق أفضلية الأسلوب الإلكتروني من خلال تجنب العيوب، وحل المشكلات التي كانت ملازمة للعمل اليدوي، وان ما يحقق الثقة به هو الشعور بالأمان والإحساس بالخصوصية، وتوفير حماية المعلومات وسلامتها، ووجود مستوى من الأمنية.

وترتكز عملية التحول إلى الحكومة الإلكترونية على قيام التعاون الكامل بين المؤسسات وعلى التفاوض واتخاذ القرار، وهذا يحتاج إلى تعاون مرن وكفء، ويرتكز على بناء قاعدة أمنية موثوقية للمعلومات لتبادلها بين القطاع الخاص وقطاع الدولة والمواطنين.

السرية في الحكومة الإلكترونية

على الرغم من كل ما يقدمه عصر المعلوماتية في الوقت الحاضر من امتيازات وخدمات، إلا أن هنالك تحديات كبيرة تنصب في اغلبها على المعلومات (سرية المعلومات) سواء كان ذلك يتعلق بحفظ المعلومات وتخزينها إلكترونياً أو المحافظة على سريتها بين المؤسسات أو التأكد من وجود المعلومة المطلوبة وإتاحتها للجميع بشكل متساوٍ. وتؤكد العمليات البينية المؤمنة لسرية المعلومات على أهمية عدم اطلاع العابثين على المعلومات المتبادلة بين قطاعات الحكومة وبين القطاع الخاص، والحكومة، والمواطن، علماً بأن معلومات الحكومة متاحة للجميع،

ولكن تحت شروط وسرية خاصة، وتعتبر سرية المعلومات هي الأولى في الاهتمام عند تطبيق الحكومة الإلكترونية بكل مراحلها .

وتتضمن سرية المعلومات على محاور متنوعة، منها السرية، والتكامل، وتوفير المعلومات، ومعرفة تاريخ دخول أي شخص إلى المعلومات وأمان المعلومات. وحتى نستطيع تحقيق السرية؛ فإنه يجب تحديد من هم الأشخاص المخولون بالدخول، وتحديد من هم غير المخولين ومنعهم من الدخول. أما التكامل؛ فهو يركز على أن المعلومات محصنة ضد التغيير سواء كان من الداخل أو الخارج. في حين يعني توفير المعلومات أنها متوافرة ومتاحة، ويمكن الاستفادة منها والحصول عليها دون أن يتم الاعتراض أو الامتناع عن إعطائها بالكامل، أو حذف جزء منها، وهنالك تفاوت في أهمية هذه المحاور لكل منظمة، إذ تعتبر سرية المعلومات أهم المحاور التي تهدف إلى تحقيقها الجهات العسكرية، أما قطاع التجارة فإنه يركز على تكامل المعلومات، فكل منظمة حسب نوع عملها وحساسيته تركز على محور، أو عدد من المحاور في الوقت نفسه.

وتعتمد سرية المعلومات والقدرة على تحقيق مستوى عالٍ من الأمان على مقدار التزام المنظمة بتوفير مفاتيح السرية، وهي:

1-**التخويل:** هو التعريف بمن يدخل إلى النظام بطرق عدة إما عن طريق كلمة السر، أو عن طريق الأجهزة، أو البرمجيات، أو من خلال استخدام الأساليب الحيوية مثل قزحية العين أو بصمة الإصبع.

2-**السيطرة على الدخول:** وتعني تحديد الجهات والأشخاص والمؤسسات المخولة المعنية بالدخول إلى النظام والسماح لهم بالدخول.

3-**التدقيق:**هو مجموعة الإجراءات التي يتم من خلالها التأكد من النظام ومدى صلاحيته، وما هي الثغرات التي توجد فيه.

ومن أكثر المشاكل التي تواجه سرية المعلومات وأمنها هو توافر أكثر من أسلوب في الدخول إلى النظام، إذ ان وجود أكثر من منظمة، أو دائرة، أو مواطن، الراغبين في الدخول إلى النظام والحصول على المعلومات مع نظام أمن غير متجانس، يجعل الأمر اكثر تعقيداً . كما تختلف أنظمة الأمان من دائرة لأخرى.

ويؤدي هذا إلى تعطيل الحصول على المعلومات حتى في هــذه الــدوائر نفســها، ولمعالجة هذه الحالات لا بد من إعادة النظر في سياسة الأمنية المتبعة بحيث تواكب التطورات في مجال أمن المعلومات.

كما تشكل الاختراقات من داخل المنظمة أو من خارجهــا مشــكلة تــؤرق الحكومة الإلكترونية، ويجب التصدي لها بتطوير أنظمة عديدة معقدة لإدارة ســلامة المعلومات وأمنها، وتحقق درجة من الأمنية لمختلف مستويات السرية للمعلومــات (سري؛ وسري للغاية؛ أو محدود السرية). كما انه لا بد من سن قــوانين رادعــة للمتطفلين، والمحترفين، والمخترقين، والقراصنة. (الزعبي ، 2002،(41-43))

جهود بعض الدول المطبقة لمشــروع الحكومــة الإلكترونيــة علــى صعيــــد الأمنيــــة (العزام، 2001،(33-48)).

نظراً لأهمية تحقيق الأمنية والخصوصية لمشروع الحكومة الإلكترونية، فإن أغلب الدول الراغبة والمتبنية لهذه الفكرة بذلت جهوداً كبيرة على مستوى عــالٍ من الاهتمام بموضوع الأمنية.

تجربة الحكومة الأمريكية: كان الهاجس الرئيسي في تطبيق الحكومة الإلكترونية في أمريكا هو أمن المعلومات وخصوصيتها، من أجل ذلك قامت الحكومة بتنفيــذ مــا يعرف بـــ(P K I- Solutions)، إذ تركز هذه التكنولوجيا على استخدام التشفير والترميز للمعلومات، وذلك لإتمام الاتصالات بين الدوائر الحكوميــة مــع بعضــها البعض، وما بين الدوائر الحكومية والمواطنين والقطاع الخاص، بحيــث يصــعب تعرف غير المخولين وغير المعنيين على المعلومات عند تشفيرها. كما تــم توقيــع عقود مع مقدمي خدمات تكنولوجيا المعلومات لتزويد الموظفين الحكوميين بشهادات الدخول للخدمات الإلكترونية.

أما على مستوى التجربة الأسترالية؛ فقد تم وضع معايير مهمة وتحديــد خطــوط عريضة على صعيد الأمنية أهمها: دليل الخصوصية للحكومة الاتحادية، وحكومات الولايات الأسترالية، وتعليمات سرية الاتصالات الأسترالية، واستراتيجية الحكومــة الاتحادية في استخدام تكنولوجيا ترميز الاتصالات من خلال توظيف حارس بوابــة

من أجل المحافظة على أمن المعلومات وسريتها لكل من المواطن، والحكومة، وقطاع الأعمال.

أما على صعيد تجربة المملكة المتحدة (بريطانيا)؛ فقد ألزم الكتاب الأبيض للحكومة الإلكترونية الصادر سنة(1999) بمعالجة موضوع خصوصية المعلومات والبيانات كما ستقوم الحكومة البريطانية بإصدار دليل لمواضيع محددة في مجال أمن المعلومات والبيانات المتداولة على شبكة الحكومة الإلكترونية.

3-الحكومة الإلكترونية في الأردن:

من منطلق الحرص الدائم على مواكبة التطورات، وتقديم الخدمات بشكل افضل وأسرع، وأعلى جودة، وفي ضوء السعي الدؤوب نحو تحويل اقتصاد الأردن إلى اقتصاد مفتوح، بادر الأردن وعزم على التوجه نحو الحكومة الإلكترونية.

وتحضيراً لذلك، تم تشكيل لجنة ملكية خاصة من أجل دراسة واقع الخدمات الحكومية، ووضع تصورات واقتراحات مستقبلية لوضع استراتيجية شاملة للتحول نحو العمل بأسلوب الحكومة الإلكترونية، حيث تم تأليف هذه اللجنة من مجموعة من المتخصصين في مجال المعلوماتية، والإدارة من كلا القطاعين العام والخاص، وعكفت هذه اللجنة على تقديم تقرير خاص رفع إلى جلالة الملك عبدالله الثاني في أيلول(2000) .

وإذا أردنا التحدث عن فوائد الحكومة الإلكترونية، ومظاهرها، ومحتواها، أو حتى مراحلها بالنسبة للأردن؛ فهي موحدة تقريباً في كل الدول، ولا يوجد خصوصية لدولة عن أخرى، لكن التحديات ومتطلبات النجاح والجاهزية هي على الأغلب. التي تختلف من دولة إلى أخرى تبعاً لإمكانيات هذه الدولة والمحددات والصعوبات التي تعاني منها.

عزم الأردن على تطبيق الحكومة الإلكترونية لمواكبة التطورات ورغبة في الإفادة من المردودات الجمة المتوقع الحصول عليها من تطبيق الحكومة الإلكترونية، وعند بداية التطبيق على ارض الواقع واجه الأردن العديد من التحديات.

وأبرز هذه التحديات

1-المستوى المتدني لاستخدام الحاسوب: يشكل الإنترنت المفتاح الذي تدخل من خلاله إلى عالم الحكومة الإلكترونية، ونظراً لارتفاع تكاليف استخدام الإنترنت وأحياناً الجهل في الاستخدام، فإن نسبة استخدام الإنترنت لا تزيد على (1.9%) من عدد السكان في الأردن.

2-محددات البنية التحتية اللازمة للحكومة الإلكترونية: يعتبر توافر بنية أساسية من أكثر متطلبات نجاح الحكومة الإلكترونية إلحاحاً، فهي الأساس الذي تبنى عليه أغلب المتطلبات اللازمة لتنفيذ الحكومة الإلكترونية، والأردن يعاني من الجاهزية في البنية التحتية الخاصة بالاتصالات.

3-توزيع استخدام التكنولوجيا الرقمية: لا يوجد توازن في توزيع المستخدمين في جميع المناطق من الناحية الجغرافية والعمرية، إذ يتمركز المستخدمون للإنترنت والحاسوب في كل من (عمان، والزرقاء، واربد) مع وجود عدد قليل من المستخدمين في بقية مناطق المملكة، ويقتصر الاستخدام على الفئة العمرية الشابة

4-الخصوصية في مواجهة الأمن: تتيح الحكومة الإلكترونية للحكومة، وكذلك للأفراد إمكانية الاطلاع على كثير من المعلومات هي في عداد خصوصيات الأفراد والمتعلقة بحياتهم الشخصية، وهذه المعلومات بحاجة إلى عناية وحماية من الدولة لتحقيق استقرار وأمن ليس معلوماتياً فقط لكن قومياً أيضاً.

5-محدودية المهارات في استخدام تكنولوجيا المعلومات: يحتاج تفعيل الحكومة الإلكترونية واقعياً والقدرة على استخدامها ونجاحها يحتاج إلى مستخدمين متمرسين على استخدام الحاسوب، وتحاول الحكومة الأردنية جاهدة نشر ثقافة معلوماتية لتكنولوجيا المعلومات والحاسوب من خلال اعتبار الحاسوب مادة أساسية تدرس في المدارس والجامعات منذ المراحل الأساسية كإجراء لمحاربة الأمية في تكنولوجيا المعلومات.

6-نقص الإطار التشريعي : إن مشروع الحكومة الإلكترونية حديث نوعاً ما، وهو بحاجة إلى تحديث، وتطوير، واستحداث تشريعات، وقوانين، وأنظمة وإجراءات خاصة تحميه وتوفر له كياناً مستقلاً ذا شرعية، ويكون محمياً من أي

تهديدات قد يتعرض لها. وفي الأردن ما يزال التشريع المتعلق بشأن الحكومة الإلكترونية في طور النمو.

7-نقص الإدراك لمفهوم الحكومة الإلكترونية: يعاني المواطن الأردني من سوء فهم، واحياناً نقص وعي وإدراك لفكرة الحكومة الإلكترونية، الأمر الذي يتطلب من الحكومة باستمرار عقد الندوات، والمحاضرات حول الحكومة الإلكترونية لترسيخ المفهوم وتوضيحه. (العزام ، 2001،(49-51)):

أمن الحكومة الإلكترونية الأردنية :

نظراً لحداثة تجربة الأردن في ضوء الحكومة الإلكترونية؛ فإن أي قضية مرتبطة بالحكومة الإلكترونية هي ما تزال في طور النمو، والأمن أحد هذه القضايا إذ يعتبر إصدار المركز الوطني الأردني لسياسة أمن المعلومات وحمايتها عام (1998) من أبرز ما أنجز على الصعيد الأمني.

وكذلك "كان الأردن قد أقر قانون حماية حقوق الملكية الفكرية عام (1992) وأجرى عليه تعديلاً عام (1998)، بحيث اصبح يتضمن مواد جزائية لتعزيزه وحذفت منه متطلبات التسجيل الإلزامية، واصبح نسخ مواد محمية بقانون حماية حقوق الفكرية، أو توزيعها دون تفويض عملاً غير قانوني بموجب القانون؛ وبالتالي فانه لا يجوز صنع أي نسخ أخرى دون تفويض صريح من صاحب حق الملكية الفكرية" (الخطيب، 2000،19).

جاهزية التحول للحكومة الإلكترونية

أما عن مدى جاهزية الحكومة الإلكترونية الأردنية للتحول نحو الحكومة الإلكترونية، فقد قام الأردن على مستوى توفير البنية التحتية بإنشاء أربع شبكات اتصالات:

1-شبكة مركز المعلومات الوطني، يرتبط من خلالها (113) دائرة ومؤسسة حكومية.

2-شبكة اتصالات سلاح الجو الملكي، التي تمتد من الوسط (عمان – المفـرق) إلى جنوب المملكة – العقبة.

3-شبكة اتصالات القوات المسلحة الأردنيـة، التي تغطي حوالي (80-90%) من المواقع الجغرافية في المملكة.

4-شبكة اتصالات الأمن العام، والتي تربط المدن الرئيسية والبلديات في المملكة من خلال حوالي (200) مركز أمني منتشرة في مختلف أنحاء المملكة.

ونلاحظ من الشبكات السابقة التي ترتبط بها المملكة غلبة الطابع العسكري عليها. لذلك فنحن بحاجة إلى شبكة اتصالات مدنية وهذا ماتعتزم شركة الاتصالات الأردنية القيام به، إذ أنها تعمل على تنفيذ مشروع شبكة الاتصالات الوطنية بكلفـة إجمالية تقدر بحوالي (7) ملايين دولار.

أما عن الإمكانيات الأخرى بوصفها مؤشرات للجاهزية، فان هنالك (82) مؤسسـة تستخدم نظم المعلومات، وهنالك (394) (Server)، و (8833) جهـاز حاسـوب بأنواعه المختلفة. وهذه الأجهزة والمعدات لازمة لتكنولوجيا المعلومات، وهنـالك (77) شبكة محلية، و(48) شبكة كبيرة، و(74) إشتراك إنترنت، و(44) موقعـاً إلكترونياً للدوائر الحكومية على شبكـة الإنترنت، وهـو في تزايد يومـاً بعـد يوم.(الزعبي، 2003،(101-102))

التهديدات الأمنية (المفهوم)

التهديد يعني احتمالية حصول خطر وأذى، وهو مجموعه مـن الاحتمـالات والأحـداث التـي تلحـق أذى بـالآلآت التقنيـة والإتاحيـة والسـرية لـنظم المعـلومات.(Timothy R & Ronald E , 1996,1)

كما عرف التهديد بأنه " هو الخطر المحتمل الذي يمكن ان يتعرض له نظـام المعلومات وقد يكون شخصياً كالمتجسس أو المجرم المحترف والهاكرز المخترق أو شيئاً يهدد الأجهزة والبرامج والمعطيات أو حدثا كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية "(عرب،2002، 84).

وسنتناول "التهديدات الأمنية"من خلال ما يلي:

أولاً:مصادر التهديدات الأمنية ثانياً:جرائم الحاسوب وتهديدها لأمنية المعلومات.

أولاً:مصادر التهديدات الأمنية.

ومصادر التهديد متنوعة منها ما يعتبر مصدر تهديد داخلي من داخل المنظمة، ومنها ما هو خارجي من خارج هذه المنظمة فحصول التهديد بشكل فعلي وليس توقعه يساهم في تحديد ومعرفة ما هو المصدر المسبب له والذي دعم حدوثه ووقوعه، وبعدما يتم تحديد مصدر التهديد يصبح بالإمكان السيطرة عليه ومعالجته أو التخفيف من حدته. ولأن الهدف من تحديد مصدر التهديد هو توفير حماية لنظام معلومات المنظمة، فلا بد من تحديد ذلك المصدر ثم إيجاد وسائل أمنية لكل مصدر واحياناً تكون هنالك عوامل مساعده على حدوث التهديد ربما هي اكثر خطورة من التهديد نفسه، لأنها تعد المسؤول الأول عن حدوث التهديد الحقيقي . (Timothy R & Ronald E , 1996 ,(1-9))

1-**مهددات الأمنية الداخلية** : وتصنف مصادر التهديدات الأمنية الداخلية إلى صنفين رئيسين :-

أ-**تقنية Technicality**

تعد الأخطاء التقنية من التهديدات الداخلية للأمنية والتي تهدد أمنية نظام المعلومات ومن أكثر الأخطاء التقنية شيوعاً حصول أعطال في الأجهزة أو أخطاء في البرامج .

ومن المثير للانتباه أن الأخطاء التقنية هي التي حظيت بأكبر حصة من بين أسوأ الأخطاء التي يرتكبها المستخدمون لأنظمة المعلومات، إذ هنالك العديد من تلك الأخطاء التي تشكل تهديداً كبيراً على أمنية انظمة المعلومات، وأبرزها.(سالم،2000، 56)

1-تسهيل ارتباط الأنظمة بالإنترنت قبل تشغيل أنظمة الحماية.

2-ربط الأنظمة التي يتم اختبارها بالإنترنت باستخدام كلمات مرور وحسابات افتراضية .

3- عدم القيام بتحديث الأنظمة عند اكتشاف فجوات ثغرات أمنية فيها .

4- استخدام بروتوكولات غير مشفره مثل (Telent) عند إدارة الأنظمة .

5- التصريح بكلمات مرور المستخدمين عبر الهاتف أو تغيير كلمات المرور بناءً على طلب الأفراد عبر الهاتف ومن قبل أفراد لا يتم التحقق من هويتهم .

6- عدم الاحتفاظ بنسخ احتياطية واختبارها .

كما أن الاستهانة بالمخلفات التقنية أمر بالغ الخطورة، إذ قد يقوم المهاجم بتفتيش المخلفات التقنية الخاصة بالمنظمة الموجودة في القمامة والمواد المتروكة كمخلفات بحثاً عن أي شئ يساعده على اختراق النظام، مثل الأقراص الصلبة المرمية بعد استبدالها، أو الأوراق التي دون عليها كلمات السر أو أسماء الملفات والبرامج.(عرب ، 2002 ، (89 – 90)).

وحتى نواجه هذا الخطر والتهديد لابد من التقيد بالوسائل الفنية التي تساعد في حماية أنظمة المعلومات وتعمل على الوقاية من هذه الأخطاء والأخطار. ومن أهمها توفير برمجيات ضبط الوصول إلى المعلومات، وحماية بوابة الدخول لنظام المعلومات، والاهتمام بنظم الإنذار، والتشفير، ومولدات كلمات السر مع ضرورة الاهتمام بالحراسات الفنية، والإجراءات المضادة، وحماية المواقع، وكذلك لابد من الحرص على عمليات تشغيل الاتصالات وصيانتها .(حسين ، 1999 ، (217 – 218)) .

ب-بشرية Humanrace

المصدر الداخلي الثاني المسبب للتهديدات الأمنية هو الأخطاء البشرية، فعند إطلاق مصدر داخلي على الخطأ البشري، يكون المعني بذلك هم الموظفون والعاملون في المنظمة، إذ يشكل الموظفون ما نسبته (75 –80%) من مصادر التهديدات الداخلية في المنظمة وتشمل هذه الفئة الموظفين الحاليين والسابقين.(البداينه ، 2002، 40) .

وعلى الأغلب تتم الأخطاء البشرية الداخلية الحاصلة من قبل الموظفين لأحد سببين، إما لأنهم غير ذي ثقة، فيكون خطاؤهم هنا مقصوداً ومتعمداً، إذ يقوم الشخص بتسريب معلومات أو إحداث ضرر لكي يستفيد هو مادياً لصالح جهة ما (عميل) أو انتقاماً منه لأنه متضرر من عمله وغير حاصل على حقوقه أما السبب الثاني فيكون إهمالاً من الشخص وعدم معرفته بأنه يرتكب خطأ. وهنا يكون خطاءً بشرياً غير مقصود وغير متعمد، ويختلف مقدار وحجم الضرر المترتب على الخطأ

البشري الداخلي حسب نوعية تخصص الفرد الذي قام بالخطأ. فكلما كان على درجه من الخبـــرة والتخصص كان حجم الضرر أكبر في حالات الخطــأ المقصـــود. (Joseph c ,1995 , (1- 6)) .

لقد أصبحت الكثير من المنظمات حذره من العنصر البشري لديها، وأخـــذت تراقب الاتصالات الهاتفية التي يجريها موظفوها، وتقوم بعمليات مراقبـــة دوريـــة منتظمة وعشوائية على الموظفين، كما يتم تدقيق تاريخ الموظفين قبل عملية الاختيار والتعيين والتأكد من مؤهلاتهم وخبراتهم حيث يتم رفض طلبات من يثبت الكذب أو التزوير في معلوماته . (البداينه ، 2002، 324) .

ومن منطلق أن العنصر البشري أثمن ما تمتلكه المنظمة، وأن الخطأ النـــاتج عن العنصر البشري من أخطر التهديدات، فهنالك جمله من التوصـــيات للمحافظـــة على آمن الأفراد والتزامهم بالأمن.(داود ، 2000 ،(49 – 51)).

1-تنظيم ومتابعة تسجيل حركة الموظفين، دخولاً وخروجاً، للمبنى وكذلك حـــركتهم الداخلية في المبنى نفسه.

2-مراقبة اتصالات المستفيدين من الخارج مع الموظفين، ومتابعة استخدامهم للنظام مع الحرص على متابعة سجل عمليات المستفيدين.

3- تحديد الإجراءات المتبعة في حالة الاستقالة أو إنهاء الخدمة أو تغييـــر مجـــال العمل مع بقاء مسؤولية الموظف الذي استقال أو أنهى خدمته عن أسرار المنظمـــة، والحرص على تغيير كلمات السر، وتحديثها بشكل دوري.

4- اختيار الموظفين بحرص شديد وإجراء تحريات عنهم وعن ماضيهم الـــوظيفي مع الحرص على عدم إعطاء الموظف حديث التعيين صلاحيات عاليـــة لاســـتخدام النظام .

5- أن يكون لدى مسؤول الأمن لنظام المعلومات في المنظمة نظـــام آلـــي يحـــدد الأشخاص كافة المصرح لهم باستخدام النظام ومستوى صلاحية كل موظف منهم .

6- ضرورة القيام بشكل دوري بعقد دورات تثقيفية وحملات توعية للموظفين حول الأمن وأهميته، وما هي التهديدات الأمنية والإجراءات المضـــادة، وحـــول إســـاءة

الاستخدام، والأخطاء الحاصلة عن طريق الموظفين بقصد أو بغير قصد، مع بيان حجم الضرر الذي يلحق بالمنظمة وبهم من جراء ارتكاب هذه الأخطاء .

2- مهددات الأمنية الخارجية: وتصنف مصادر التهديدات الأمنية الخارجية كالتالي:

أ-الكوارث الطبيعية Natural Disasters

تعني الكارثة "أي حادث ينتج عنه تعطيل نظام الحاسب عن العمل لمده محسوسة " ويحمل مفهوم الكارثة من وجهة نظم تقنيات المعلومات خصوصية للمفهوم، ومن أشهر الكوارث الطبيعية على صعيد العالم زلزال سان فرانسيسكو، وانقطاع الكهرباء الشامل عن الرياض، وفيضانات بنجلاديش، وإعصار أندرو. واكثر ما يتضرر أثناء حدوث الكارثة في مجال تقنية المعلومات هو النظام الذي ينهار في أغلب حالات الكوارث.(داود ، 2000 ، 93) .

وتتعرض نظم المعلومات إلى تهديد طبيعي ناتج عن الكوارث الطبيعية مثل: (الحرائق، والهزات الأرضية، والبراكين، والزلازل، والفيضانات) وتهديدات طبيعية ذات صبغة بيئية مثل (الكهرباء، والحرارة، وأنظمة التبريد) ولا يقتصر الضرر الناتج عن الكوارث الطبيعية على خسارة المعدات والأجهزة فقط بل يتعداه إلى حدوث فقدان في المعلومات والبيانات والبرمجيات فالنظام بأكمله هو عرضة للتهديدات.(البدانيه ، 2002 ، 351).

وكون الخطر المحتمل حدوثه نتيجة الكوارث يلحق الأذى بأحد النظم أو الأنشطة على شكل إفشاء المعلومات، وتعديلها، أو فقدانها، أو تدميرها، فلا بد من عمل دراسة وافية لمحيط العمل، وطبيعته، ونوع الأجهزة والمعدات المستخدمة في المنظمة، وشبكات نقل البيانات والبرمجيات المستخدمة، ودراسة تدقيق البيانات داخل المنظمة وادارتها وكذلك بين المنظمة والجهات الخارجية، ودرجة تأمين النظام بمجمله، وذلك من أجل تحديد نقاط الضعف فيه، والقدرة على تحديد احتمالات الأخطار، ولابد لأي منظمة من أن تكون مستعدة لمواجهة ومعالجة الكارثة، أي أن تكون لديها القدرة عند حدوث الكارثة على تشغيل الأنظمة الضرورية لإنقاذ العمل واستمراريته، وأن يكون هنالك خطه لمواجهة الكوارث "خطة طوارئ " إذ يساهم تخطيط الكوارث في المحافظة على ثقة الجمهور والمنظمات الأخرى بالمنظمة،

والاحتفاظ بعلاقات جيده مع الموظفين، وتقليل الخسائر المادية، وعلى الإسراع في استعادة أوضاع العمل إلى ما كان عليه، و تفادي حدوث أزمات عقب حدوث الكارثة . (داود ،2000،(96-99)).

ويمكن حماية أنظمة المعلومات في المنظمة من أخطار التهديدات الخارجية من خلال عدة وسائل منها جدار النار، ووضع عوائق تحول دون الوصول إلى أمكنة الحاسوب، ووضع منبهات للحريق، ونظم غلق تلقائية لنظم الحاسوب والقيام بالتبريد عند حدوث الحريق، وتوفير طفايات الحريق في غرف الحاسوب، ومنع التدخين في تلك الغرف، والاحتياط عند حدوث برق أو صواعق من خلال إطفاء الحواسيب، والمحافظة على درجة حرارة بين (10 – 26) درجة مئوية، وان تكون نسبة الرطوبة في غرف الحاسوب بين (35 – 50%)، ومن المستحب استخدام منظم كهرباء لتفادي حالات عدم استقرار التيار الكهربائي (البداينه ، 2002 ، 351) .

ونظراً لأن الكوارث الطبيعية خارجة عن الإرادة البشرية، وغالباً ما يكون فيها الدمار شاملاً وكبيراً، فإن التعاون بين الحكومة والقطاع الخاص والقطاع التطوعي ينبغي ان يكون قائماً في إعادة الخدمة وإصلاح الأعطال.(البداينه ، 2002 ،339).

ب-المحترفون والقراصنة Professionals and Hackers

تسميات عده أطلقت على مصدر التهديد البشري الخارجي (المخترقون ، والمحترفون ، والهاكرز ، والقراصنة) ورغم أن جميع هذه التسميات تشترك في إحداثها للتهديد والضرر على المنظمة والنظام المعلوماتي، إلا انه توجد هناك بعض الفروق بينها .

المخترقون وتاريخهم.(عبد النبي ،2003، (1-6))

(هم الجماعة الذين يملكون الخبرة في البرمجة ومعالجة الشبكات ولهم المقدرة على اتخاذ الإجراءات التقنية للسعي إلى تخطي الحواجز الموضوعة لحماية الشبكات وأن تنمية قدراتهم تعود إلى ممارستهم الطويلة وخبراتهم الواسعة في استيعاب لغات البرمجة وأنظمة التشغيل) فهنالك المخترق (Hacker) وهنالك(Cracker) فالهاكرز هو الشخص الذي يتمتع بخبرة عالية ومعرفة واسعة في لغات البرمجة، وأنظمة التشغيل، والتحليل، والتصميم مما يمكنه بأن يكون خبيراً

فهو يريد أن يثبت قدراته التقنية والفنية، ولا يحمل دوافع تخريبيــة أو حاقــدة أمــا الكريكر؛ فهو المستخدم العادي أو الهاوي الذي يســعى إلــى اختــراق الأجهــزة والتلاعب بالمعلومات المخزنة، وتعكس اعتداءاتهم ميولاً إجرامية هــدفها إحــداث التخريب.

ويرجع تاريخ المخترقين في الشبكات إلى الستينات، إذ كان يطلــق علــى المبرمج المتمكن الذي يقوم بتصميم البرامج بسرعة بالمخترق، وكان من أشهرهم: (دينيس، و ريتستي، و كيت تومسون) وذلك بسبب قيامهم بتصميم برنامج (UNIX) وكان ذلك سنة "1969" ويعتبر أسرع برنامج مصمم في وقتــه ، وكــان العصــر الذهبي للمخترقين خلال الفترة من عام (1980 –1989) وذلك عقب إنتاج الحاسوب الشخصي(IBM(1) إذ ظهرت في أمريكا مجموعتان همــــا مجموعــة(LOD) و(MOD) وقام التنافس بينهما عام "1984" واستمر هذا التنــافس أربــع ســنوات، وانتهى بالقبض عليهما بعد عام "1990" كما ظهرت مجموعات من المخترقين فــي أمريكا متخصصة في سرقة بطاقات الائتمان تؤثر على الأمن والخصوصية .

أما المحترفون؛ فهم أصحاب سعه في الخبرة والإدراك للمهــارات التقنيــة ويتميزون بالتنظيم والتخطيط للأنشطة التي ترتكب من قبلهم، والهدف من اعتداءاتهم هو تحقيق الكسب المادي لهم أو للجهات التي يتم الاعتداء لصالحها، كما قد يكــون لبعضهم أهداف سياسية تتمثل في التعبير عن موقف فكري أو فلســفي أو نظــري. وتتسم هذه الفئة بالتكتم وعدم تبادل المعلومات بشأن أنشطتهم .(عرب ، 2002 ، (282 – 283)) .

أشكال الاختراق وأعراضه :

ويشتمل اختراق المعلومات على شكلين هما: اختــراق المعلومــات الثابتــة واختراق المعلومات المتحركة أو المنقولة. وللاختراق أي كان نوعه مجموعه مــن الأعراض أهمها(اللهو، والتعطيل، والتخزين، والتدمير، والتجسس، والسطو علــى الأموال). (زكي ، 2001، 57) .

وكون الهاكر هو الشخص صاحب الخبرة، والمعرفة فإنه يشكل خطراً وتهديداً كبيرين. لذلك لابد من معرفة مبادئهم وأهم الأفكار التي يؤمنون بها، ومن أبرز الأفكار التي يتبناها الهاكر.(سالم ، 2000 ،(56 – 57)) .

1-الحرية في تبادل المعلومات، إذ يتميز الهكره باقتناعهم وإيمانهم العميق بعدم وجود سبب مقنع لحجب المؤسسات الخاصة والحكومية معلوماتها عنهم، و يؤمنون أيضاً بأن المعرفة التقنية هي ملك للبشرية، ويجب أن تكون متاحة للجميع بحرية، وهذا ما يدفعهم إلى القفز فوق كل حاجز يحجب المعلومات عنهم.

2-العمل بروح الفريق واحترام إنجاز الآخرين مهما كان بسيطاً والبدء من حيث انتهى الآخرون، ويجب تقدير إنجازهم واحترام إبداعهم التقني، وهذا الأسلوب يساعدهم على سرعة الإنجاز والتطوير .

3-ضرورة المشاركة في المعرفة التي يتوصل إليها الهاكر، إذ يعتبر أكثر الهكره نجاحاً ذلك الذي يساهم بتقديم معرفته التقنية بشكل مجاني دون مقابل.

4-التحلي بالصبر والمثابرة وامتلاك الثقة بالنفس من أجل مواجهة المشاكل والتحديات المتزايدة في عالم تقنية المعلومات، وكذلك من أجل دراسة هذه المشكلات والقيام بالأبحاث، وإبراز الإبداعات، والمواهب، والخبرات التي يمتلكها الهكره .

5-الابتعاد عن الرتابة والروتين حتى لا يقتل الإبداع لديهم فكلما امتلك الإنسان القادر على الإبداع مساحة أوسع للتفكير زاد مستوى إبداعه وابتكاره .

وفي إحصائيات وردت في تقرير أعده اتحاد منتجي برامج الكمبيوتر، تبين أن هنالك انخفاضاً في نسبة القرصنة في مجال برامج الحاسوب في الأردن خلال الفترة بين عام (1994 –1997) من (87% – 80%) كما أشارت الإحصائيات إلى أن منطقة الشرق الأوسط وأفريقيا هي ثاني أكبر المناطق التي تتركز فيها أعمال القرصنة في العالم، إذ بلغت ما نسبته (65%) حسب إحصاءات الاتحاد، وأن اكثر الدول تعرضاً لأعمال القرصنة هي: (الولايات المتحدة، والصين، واليابان، وألمانيا، وبريطانيا، وكندا، وروسيا) وتقدر خسارة هذه الدول بحوالي (7) مليارات دولار أي ما نسبته (76%) من إجمالي حجم الخسارة الكلية على مستوى العالم.(الخطيب ، 2000 ،19) .

ومهما كان مصدر التهديد البشري، سواء أكان داخلياً أم خارجياً، فإنه لابد من نشر التوعية على الصعيدين الداخلي والخارجي للمنظمة وعلى مستوى الدولة عبر الإعلام بشتى وسائله، ومن خلال دعم الدعاية والإعلان حول التهديدات والقرصنة، ومخاطرها، وآثارها على جميع الأطراف، ولابد أيضاً من التحلي بأخلاقيات العمل الأمني من قبل رجل الأمن والحماية في المنظمة والعاملين بشكل عام، والتعامل بحذر شديد مع تجار التكنولوجيا ومع القراصنة أنفسهم، لتفادي وتجنب التصرفات غير الأخلاقية لهؤلاء القراصنة. ويقدم القراصنة، على الأغلب على أعمال الاختراق والتخريب أملاً في أن يكونوا من أصحاب السلطة العليا في المنظمة أو مستشارين لها، لكن وضع المنظمة جملة من الشروط للتوظيف أهمها وأكثرها حساسية هو توافر السمعة الاجتماعية والوظيفية الجيدة وخلو الملف الوظيفي من ارتكاب جرائم ترتبط بعملة وجرائم بشكل عام، كلها شروط رادعة للقراصنة عن القيام بأعمالهم التخريبية، وعدم الإقدام على القرصنة؛ لأنها ستكون سبباً في رفض طلب توظيفه في تلك المنظمة، ومن ثم فإنه لن يصبح مستشاراً بسبب عدم نظافة ملفه الوظيفي والاجتماعي(Donn B , 1996, (1 –6))

ج-البرمجيات الخبيثة (Malicius Code)

"هي مجموعه متنوعة ومختلفة من البرمجيات التي تستغل للتدمير سواء تدمير النظام أو البرمجيات أو المعطيات أو الملفات أو الوظائف أو تستثمر للقيام بمهام غير مشروعه مثل الاحتيال أو غش النظام وتختلف على الأغلب هذه البرمجيات عن بعضها البعض من حيث التركيبة، أو أسلوب الهجوم، أو طريقة أحداث النتائج، ومن هذه البرمجيات (الفيروسات، وحصان طرواده؛ والقنابل المنطقية؛ والديدان).(عرب ،2002،100)

ولتمييز هذه البرمجيات عن بعضها البعض، سنقوم بتناولها مع أهم الخصائص لكل نوع:

الفيروس : (Viruse)

هو برنامج أو مجموعة تعليمات وأوامر للحاسوب الآلــي، يهدف توجيه الحاسوب إلى القيام بأعمال لم يطلبها منه المستخدم، وغالباً ما يكون هدف هذه الأعمال هو إفساد المعلومات، أو حذفها، أو إعاقة نظام الحاسب الآلي، أو تعطيله،

أو استغلال مصادره لغير ما خصصت له، أو أحياناً لمجرد عرض عبارة أو رسمه على شاشة العرض لغرض ما يقصده كاتب برنامج الفيروس. (الشايع ، 1990 ، 19) .

حصان طرواده (Trojan Horse)

يعبر هذا البرنامج عن العملية التي بقدر ما تمتاز بالبساطة بقدر ما توصف بالخطورة، فبينما يقوم مستخدم الجهاز بتشغيل برنامج ما، وهو منبهر من الرسومات الرائعة التي تظهر أمامه على الشاشة التي أحياناً تصاحب بموسيقى من خلال ميكرفون النظام يقوم البرنامج بإعادة تشكيل وحدة إدارة الأقراص الصلبة بالكامل بطريقة غير ملحوظه، إذ يظهر البرنامج كما لو أنه يؤدي بعض مهامه المفيدة لكنه في الحقيقة يتضمن في داخله بعض الأوامر التي تؤدي مهام غير متوقعه مثل محو ملفات مخزنة . (بركات وابراهيم ، 1990 ، 30) .

القنابل المنطقية (Logic Bombs)

هو برنامج يؤدي إلى الإفساد والتدمير عند توافر مجموعة من الشروط، إذ يكون مبرمج التنفيذ وفقاً لحصول حدث ما أو شرط معين مثل أول شهر أو سنة ما أو مرتبطاً بظهور رقم معين مثل الرقم الوطني لشخص ما. وتحتاج القنبلة المنطقية إلى برنامج مصنف لحمل برنامج القنبلة والى حين حصول الحدث الذي يعتبر شرط الانطلاق يكون حدث التزنيد للقنبلة ويبدأ التنفيذ، وقد تعدل هذه القنبلة بيانات أو تشطبها؛ أو تشطب ملفاً كاملاً بشكل كلي، أو توقف الجهاز، أو تقوم بنوع آخر من أنواع التدمير .(حسين ، 1999 ، 156) .

الديدان (Worms)

هي مجموعة من التعليمات التي تبحث عن الجزء غير المستخدم من الذاكرة ثم تقوم بنسخ نفسها لملء هذا الجزء من الذاكرة، ومن ثم تشغل مساحة كبيرة من الذاكرة مما يعطل الجهاز عن تأدية وظائفه، ويؤدي إلى توقف النظام وهذا البرنامج يعيد إنتاج نفسه بوساطة عمل نسخ عن ذاته، وتتسلق الديدان إلى جميع مستويات نظام الحاسوب دون الحاجة إلى برنامج حامل لها.(الغريب، 1994، 47).

تاريخ الفيروسات

نظراً لأهمية الفيروسات وخطورتها وكونها أكثر البرمجيات الخبيثة انتشاراً ومعرفة لدى الناس عامة، فإنه لا بد من توافر معرفة أوسع حولها .

ويعود تاريخ بدايات ظهور الفيروسات في الحواسيب إلى نهاية الأربعينات، وقد يكون أحد الاختصاصيين في علم الحاسوب "جون فون بتونان " هو أول من فكر بأمر الفيروسات، إذ نشر مقالاً حول الفيروسات عام (1949) ثم ظهر في أوائل الخمسينات بعض عوارض الفيروسات، لكنها كانت محددة بسبب عدم ارتباط الحواسيب مع بعضها البعض، وبقي الأمر سراً حتى عام (1983) إلى أن تفشى الفيروس في أحد أهم البرامج المعلوماتية وهو برنامج (UNIX) وأحدث ضجة كبيره كما ظهرت بعض الحوادث الفردية من صغار المبرمجين الذين قاموا بزرع فيروسات في شبكات الحاسوب لشركات تتعامل في مجالات عملية وتطبيقية حساسة.(أبو علي ، 1994 ، 14) .

أعراض وجود الفيروس

أثناء التعامل مع الحاسوب تلحظ من العوارض والمشاهدات ما يدل على وجود فيروس. ومن أهم هذه الأعراض . (أبو علي ، 1994 ، (16 - 17)).

1-البطء في تنفيذ البرامج عما كان معتاداً، وتؤثر بعض أنواع الفيروسات على وقت تنفيذ البرامج وإنجازها، وعلى إجراءات بدء التشغيل للنظام والبرامج مما يجعل تنفيذ البرامج يستغرق وقتاً أكثر من المعتاد .

2-ظهور وسائل خطأ غير مألوفة، وبخاصة الرسائل المتعلقة باستخدام الأقراص والبرامج بشكل متكرر، وهذا دليل على محاولة الفيروسات الوصول إلى هذه الأقراص والبرامج.

3-إضاءة مصابيح السواقات دون سبب ظاهر .

4-انخفاض المساحة الفارغة للتخزين على القرص دون سبب ظاهر، وهذا دليل على بدء تناسخ الفيروسات .

5-اختفاء الملفات وظهورها بشكل غامض، وهذا دليل على بدء نشــاط الفيــروس وعمله التخريبي بحذف ملفات، واحياناً ظهور ملفات لا مبرر لوجودها .

6-انخفاض ذاكرة النظام نظراً لاحتلال الفيروس جزءاً كبيراً من الذاكرة .

7-تغيير حجم البرامج التنفيذية التي تعتبر من أهم البرامج التي يغزوها الفيروس .

أهم طرق الوقاية من الفيروسات .

هنالك طرق عدة ومتنوعة لأغراض الوقاية من الفيروسات منها ما هو واجب على المنظمة التقيد به، ومنها ما هو من طرف الأفراد في داخل المنظمة وخارجها، لكن في النهاية تساعد جميع هذه الطرق في الوقاية من الفيروســات، وأهــم هــذه الطرق. (داود ، 2000 ، (79 – 86)) .

1-توعية المستفيد، إذ يشكل وعي المستفيد حجر الأساس في جهود الحماية ضــد الفيروسات، فوعيه بمقدار الضرر المترتب على التهديد الواقع بســبب الفيروســات يجعله أكثر حذراً وحرصاً على التقيد بالتعليمات .

2- استخدام أسلوب تعقب آثار الفيروس بحيث يمكن التوصل إلــى مصــدر هــذه الفيروس مما يجعل مروجي الفيروسات أكثر حذراً ويقظة قبل القيام بإنتــاج هــذه الفيروسات، وزراعتها، والترويج لها.

3-عدم استخدام برامج غير معروفة المصدر أو مقلدة أو منسوخة مع الحرص على التأكد من أن النسخ الجديدة مغلفة، ولم تستخدم من قبل .

4-عند إعادة استخدام أقراص مرنة قديمة لابد من تهيئتها (Format) بدلاً من مجرد مسحها (Delete) .

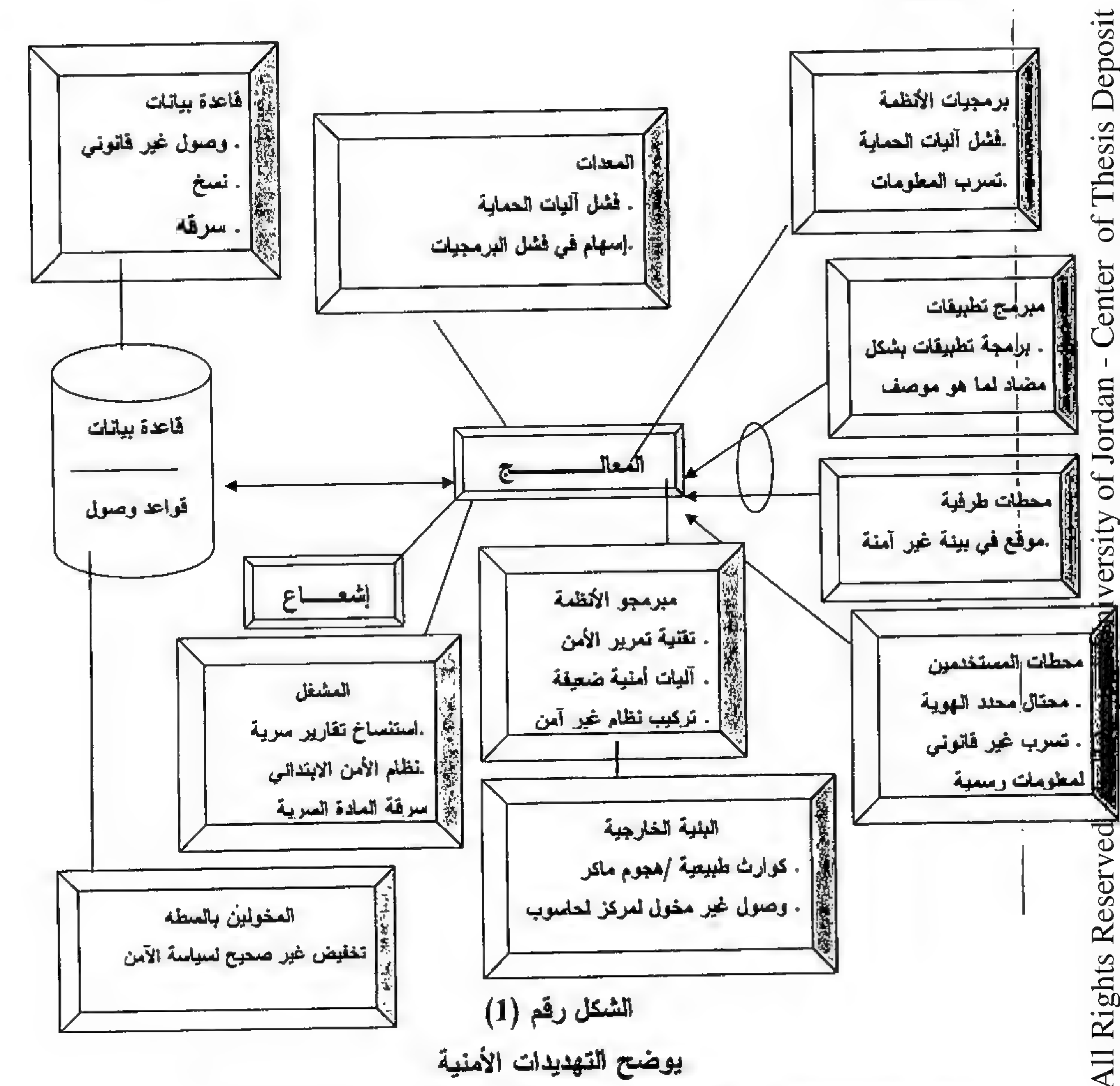
5-التأكد من أن الجهاز مغلق عندما يتم الانتهاء من استخدامه مع ضرورة الاحتفاظ بسرية كلمات المرور، وتغييرها كل فتره بشكل دوري .

6-الاحتفاظ بنسخ احتياطية من البرامج والبيانات والحرص على الاحتفاظ بها فــي مكان آمن وبعيد عن الحاسوب الشخصي .

7-الحرص على استخدام برامج مكافحة الفيروسات .

8-تدريب الموظفين على كيفية الوقاية ضد الفيروسات، وعلى كيفية التعامل معها عند العثور عليها ومعالجة آثارها .

وفي نهاية الحديث عن التهديدات الامنية ومصادرها يوضح الشكل التالي ابرز هذه التهديدات .



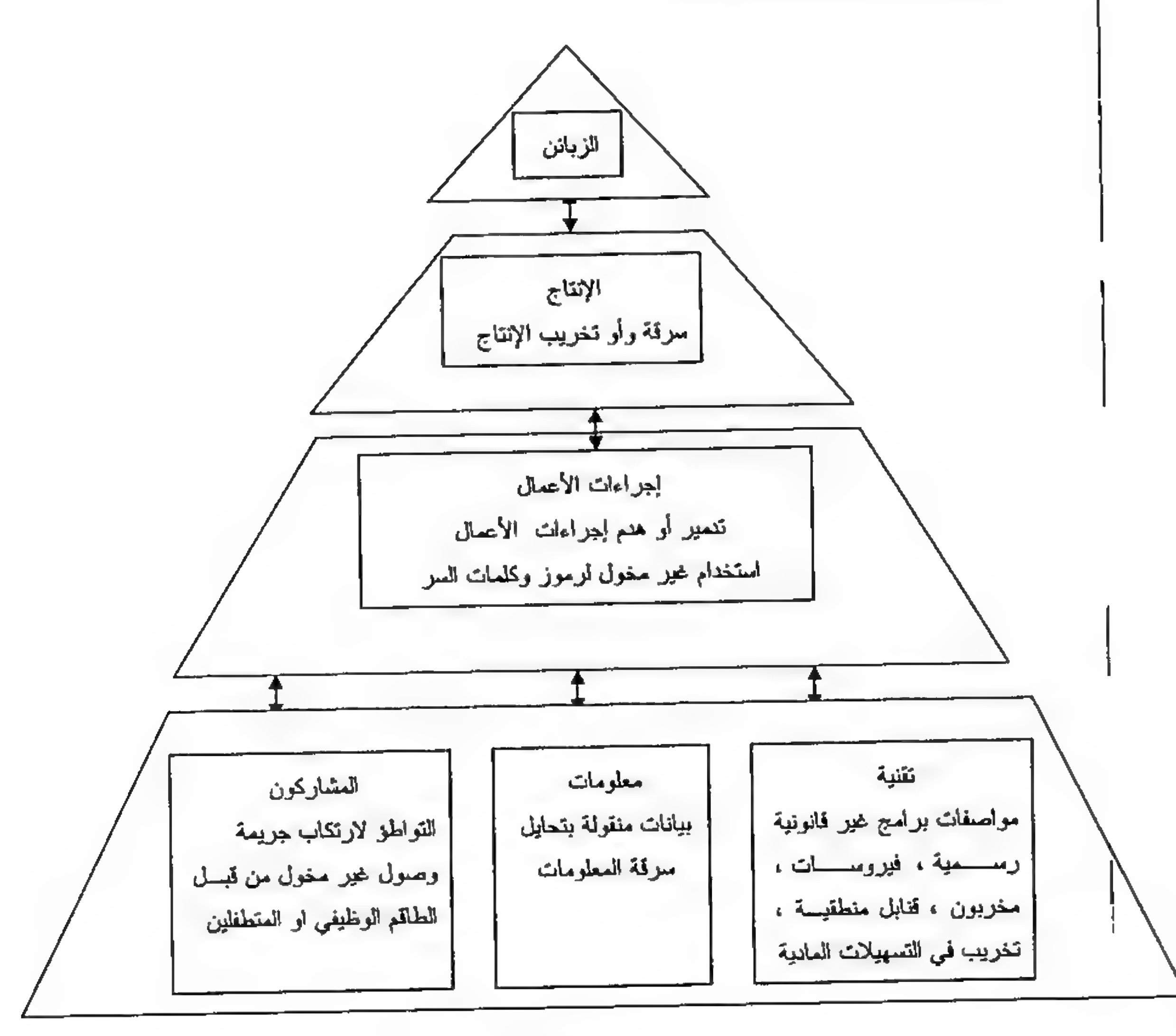
الشكل رقم (1)

يوضح التهديدات الأمنية

المصدر : (Turban, EFRAI & McLean, Ephraim & Wetherbe, James, (1999), Information Technology for Management, John Wiley & sons. Inc, New York ,p(662).

ثانياً:جرائم الحاسوب وتهديدها لأمنية المعلومات

تطرقنا في الجزء الأول إلى مصادر التهديد (مسبباته) وكانت الكــوارث الطبيعيــة والحوادث مسببات هذا التهديد التي ليس للأفراد أي دور في حدوثها. ومن ناحية أخــرى كانت هناك البرمجيات الخبيثة والاختراقات والقرصنة التي تتم بفعل فاعــل مــن داخــل المنظمة وخارجها. وتضعنا حصيلة هذه الاعتداءات والاختراقات والقرصنة والبرمجيات الخبيثة أمام جريمة سواء استخدم الحاسوب بوصفه أداة لارتكابها أو كان هو بيئة الجريمة ، ويتضح هذا من الشكل رقم (2).



الشكل رقم (2)

يوضح التهديدات المرتبطة بجرائم الحاسوب

المصـــــدر : (Alter, Steven,(1999), information systems ,Addison-Wesley Educational,Publishers Inc , p468)

ويعد هذا النوع من الجرائم حديث العهد على مستوى العالم بشكل عام والدول النامية بشكل خاص، وهذه الحداثة انعكست على التشريعات والقوانين والأنظمة المتعلقة بهذه الجرائم، فهي ما تزال في طور النمو، وتكاد تكون شبه معدومة رغم انطلاق التطورات الحاصلة في عالم المعلوماتية بخطى متسارعة جداً أما التطورات التشريعية على هذا الصعيد، فإنها لا تسير بالمستوى نفسه من السرعة، وهذا ما أحدث فجوة كانت من أكثر ما حفز المرتكبين لهذا النوع من الجرائم على التمادي فيها وارتكاب المزيد منها .

دور الحاسوب في ارتكاب الجريمة وكشفها

يؤدي الحاسوب ثلاثة أدوار رئيسة في ارتكاب الجرائم وهي :

1-أن يكون الحاسوب هدفاً للجريمة، وذلك في حالة الدخول غير المصرح به إلى النظام واختراقه، أو سرقة المعلومات، أو زراعة الفيروسات لتدمير الملفات المخزنة ومحتوياتها أو تعديلها أو في حالة الاستيلاء على البيانات المخزنة المنقولة عبر النظم .

ويعتبر تعرض السرية والخصوصية والتكاملية وسلامة المحتوى للاعتداءات من أبرز الملامح والمظاهر التي تشير إلى أن الحاسوب هدف للاعتداء .

2-أن يكون الحاسوب أداة ووسيلة لارتكاب جرائم تقليدية مثل استخدام الحاسوب للاستيلاء على الأموال بإجراء تحويلات غير مشروعه، أو باستخدام التقنيه في عمليات التزييف والتزوير وفي الاستيلاء على أرقام بطاقات الائتمان وإعادة استخدامها، والاستيلاء على الأموال بوساطتها. وقد يستخدم بوصفه وسيلة للقتل من خلال الدخول إلى قواعد البيانات الصحيحة والعلاجية وتحويرها أو من خلال التلاعب في عمل الأجهزة الطبية والمخبرية .

3- ان يكون الحاسوب هو بيئة الجريمة كما في تخزين البرامج المقرصنة فيه أو في حالة استخدام الحاسوب لنشر المواد غير القانونية أو عند استخدامه لتخزين أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية .

هذا عن دور الحاسوب في ارتكاب الجرائم، أما دوره في الكشف عنها، ففـــي ذات الوقت الذي يستخدم فيه لارتكاب الجريمة، ويكون هو البيئـــة المســـتهدفة، يـــؤدي الحاسوب دوراً لا يمكن إنكاره في اكتشاف الجريمة، إذ يستخدم على نطاق واســـع في التحقيق الاستدلالي للجرائم كافة. وكون الحاسوب يستخدم بوصفه وســـيلة وأداة لارتكاب الجريمة، فلا بد من ان يكون هو الوسيلة المستخدمة للكشف عنها، إذاً على الجهات القانونية الحرص على استخدام أحدث التقنيات؛ لاعتماد المجرمين عليها في ارتكاب الجرائم المعلوماتية . (عرب، 2002، (245-247))

وبعد الإقرار بوجود جرائم حاسوب، لابد لنا من تعريفها بأنها "هي الجريمـــة التي يتم ارتكابها إذا قام شخص ما بطريقه مباشرة أو غير مباشرة فـــي اســـتغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة ومصلحة الأفـــراد خاصة ".(محمد، 1419هـ، 49).

أنواع جرائم الحاسوب

كون الحاسوب عالماً كبيراً قائماً بذاته هو وتقنياته و الخدمات التي يقدمها في اتساع، فقد انعكس هذا التنوع والاتساع على الجرائم الواقعة عليه ويمكـــن تصـــنيف أنواع هذه الجرائم إلى ما يلي :-

1-الجرائم الواقعة على الحاسوب نفسه .

2- الجرائم الواقعة على البيانات .

3-الجرائم الواقعة على الخصوصية الشخصية ممثلة بالمعلومـــات الشخصـــية لأي إنسان، واستغلالها في حالات التهديد والابتزاز .

4-الجرائم الاقتصادية الواقعة على الأموال ممثلة بعمليـــات التزويـــر والتزييـــف والاعتداء على حقوق الملكية الفكرية مثل: القرصنة للبـــرامج؛ والاعتـــداء علـــى العلامات التجارية؛ وجرائم غسيل الأموال عبر الإنترنت، وسرقة أرقـــام بطاقـــات الائتمان .

5-الجرائم الأخلاقية المخلة بالآداب العامة مثل: نشر الفاحشة، والمساس بالحيـــاء، والمقامرة، والأنشطة الإباحية .

6- جرائم ضد الحكومات مثل نشر المعلومات العسكرية السرية، والإرهاب الإلكتروني. (خليفات ،2002،(30-31))

ولا تنحصر أنواع الجرائم على هذه الأصناف فقط ولن يقف نموها عند هذا الحد، فكل يوم هنالك تطور جديد على صعيد المعلوماتية، و يظهر تهديد يواجه هذا التطور، وينشئ جريمة جديدة .

دوافع ارتكاب جرائم الحاسوب.

تختلف الدوافع المسؤولة عن ارتكاب السلوك الإجرامي التخريبي للحاسوب ومن أهم الدوافع (عرب ، 2002 ، (289 - 292)) .

1-السعي نحو الكسب المادي.

2-رغبة الحاقدين في الانتقام من رب العمل، وإلحاق الضرر به.

3-الرغبة في إبراز الخبرات التقنية وقهر النظام، والتفوق على تعقيد وسائل التقنية.

4-دوافع سياسية أو فكريه للقيام بحرب معلومات وإرهاب إلكتروني.

5-دوافع المنافسة التي توجه السلوك نحو الاستيلاء على الأسرار التجارية.

خصائص جرائم الحاسوب :

1-وقوع الجريمة على أحد مكونات النظام المعلوماتي أو خلالها، واعتبار النظام المعلوماتي هدفاً أو وسيلة أو بيئة للجريمة أياً كانت الصورة، فنحن بصدد جريمة واقعة على النظام المعلوماتي، متعددة الصور، فقد تكون احتيالاً معلوماتياً أو قرصنه للبرامج أو تجسساً معلوماتياً، وربما تكون كل هذه الصور مجتمعة .

2-صعوبة اكتشاف جريمة الاعتداء على برامج الحاسوب الآلي، وذلك لعدة أسباب أهمها أنها جريمة هادئة لا عنف فيها، وأنها جريمة فنية لا تترك أي أثر من الآثار التي تتركها جريمة اقتحام مكان للسرقة مثلاً أو التخريب أو الاعتداء عليه، كما أنها جريمة تعتمد على تغيير الأرقام والبيانات أو محوها من ذاكرة الحاسوب الآلي .

3- صعوبات إثبات جريمة الاعتداء على برامج الحاسوب ، وذلك بسبب أنها جريمة لا تترك أثراً دالاً عليها، وأنها إذا تركت أثراً، فإنه يصعب الاحتفاظ به فنياً

أو أنها لا تترك أثاراً غير مرئية مما يجعل من الصعب على المحقق التقليدي أن يفهم حدودها الإجرامية، كما أنها جريمة مبنية على الخداع في ارتكابها والتضليل في التعرف على مرتكبها، وأنها جريمة بيضاء تعتمد على قمة الذكاء في ارتكابها .
وتعتبر صعوبة التحريات عن جرائم الحاسوب من اكثر خصائص جرائم الحاسوب خطورة، إذ يستطيع المجرم استخدام اسمه واسماء أخرى لارتكاب الجريمة نفسها التي كان قد ارتكبها عدة مرات، ومن الصعب اكتشافها. كما أن إمكانية محو أدلة الجريمة وبراهينها على الشبكات يجعل التحريات أكثر صعوبة، ويزداد الأمر تعقيداً لعدم وجود نصوص قانونية حالياً لملاحقة كل الجرائم المرتكبة على الشبكات مما يخلف مشكلة قانونية لرجال الشرطة . (شتا ، 2001 ، (78 – 103))

أثر جرائم الحاسوب في المجتمع

تشكل جرائم الحاسوب خطراً كبيراً يهدد مختلف الشرائح، أفراداً، وجماعات، إذ أن انتهاكات الخصوصية، وإفشاء الأسرار، والقرصنة، تشكل انتهاكاً لحقوق الإنسان، وتعمل على زعزعة الاستقرار الاجتماعي، وتهدد سيادة الدول، فقد أصبحت حرب المعلومات من اكثر الحروب خطورة في الوقت الراهن، ولا يقتصر ضررها على الاستقرار الاجتماعي فحسب بل يمتد إلى زعزعة الاستقرار الاقتصادي الناتج عن الكوارث المالية التي تسببها جرائم الحاسوب الآلي للأفراد والمؤسسات التجارية والحكومية كما أنها تحدث زعزعه للاستقرار السياسي والعسكري في الدولة، وذلك في حال كشف أسرار اتفاقيات بين الدول أو تفاوضات سياسة، وكذلك في حال كشف أسرار عسكرية أو التشهير بشخصيات سياسية وعسكرية. كما تعتبر جرائم الحاسوب مهدداً رئيسياً لحياة فئات من المجتمع وذلك عندما يتم الاعتداء والتلاعب في القوائم الصحية والتحكم بالأجهزة الطبية، وهي تهدد أيضاً سلامة المجتمع ونظامه الأخلاقي، وذلك عندما يستخدم الحاسوب في أغراض غير مشروعة وإباحية.(المسند والمهنيي ، 1421 ، (173 – 174)).

أهمية توفير حماية جنائية لبرامج الحاسوب .

أدى التطور السريع في المعلومات وتنوع مجالات استخدام الحاسوب إلى تنوع فرص احتمالات الاعتداء على برامجه، وسرقتها، وإتلافها، وتزويرها، واستخدامها غير مشروع، فأصبحت برامج الحاسوب محلاً لانتهاكات مدنية وجرائم جنائية عدة، الأمر الذي اقتضى توفير حماية مدنية وجنائية لهذه البرامج للحد من الظاهرة الإجرامية التي هي في تزايد واتساع مستمرين . فالحماية الجنائية لبرامج الحاسوب تحقق حماية جنائية لأسرار الأفراد ضد النشر، وتعمل على تأمين الاستثمارات المادية والبشرية المستخدمة في تكنولوجيا المعلومات، وتساهم في دعم وتشجيع الابتكار والتقدم العلمي والتكنولوجي، وفي تحقيق أهداف التنمية الاقتصادية والاجتماعية للمجتمع . (شتا ، 2001 ،(8-18)) .

ويحتم الخطر الكبير الذي يترتب على وقوع جرائم الحاسوب توفير وسائل حماية ضد هذه الجرائم، وإقرار وسن تشريعات صارمة تجاه هذه الاعتداءات المرتكبة لتكون رادعاً للمجرمين ومرتكبي هذه الأفعال التخريبية، إذ تمت الاستفادة من الكثير من القوانين القائمة بعد تعديلها لحماية الحاسوب مثل القوانين المتعلقة بحقوق المؤلف، وحماية الملكية، وبراءات الاختراع .(الطفي ، 1994 ، 25) .

أبرز المشاكل والصعوبات التي تكتنف جرائم الحاسوب وتتحقق فيها

تعد جرائم الحاسوب على اختلاف أنواعها وأشكالها، جرائم حديثة غيرت في النظرية التقليدية للجريمة، إذ تتصف هذه الجرائم بأنها جرائم ممتدة عبر الدول والقارات، ويتبع في تنفيذها وسائل حديثة. ونظراً لصعوبة إثبات الجريمة وكشفها؛ فإن هنالك عقبات عدة ومشاكل متعددة مرتبطة بهذه الجرائم، أبرزها تنفيذ جرائم الحاسوب ضمن بيئة افتراضية منطقية غير مادية من خلال أوامر وأفعال على شكل نبضات إلكترونية غير مرئية، ومن ثم لا تترك جريمة الحاسوب ومساهمة التكنولوجيا في سهوله محو الدليل أو تدميره وإعاقة الوصول إليه مجالاً لاستخدام وسائل الحماية، كما أن ضخامة تكاليف جمع الأدلة وقلة الخبرة وضعف الثقافة بتقنية المعلومات لها تأثير كبير على إثبات الجريمة.

وكون جرائم الحاسوب عابرة للدول؛ بمعنى انه قد يكون المجرم في دولـه والدليل في دوله أخرى وآثار الجريمة في دولة ثالثة. والقوانين الجنائية على امتداد الدول – كما هو معروف – مازالت تتبنى فكرة الإقليمية محدداً للاختصاص، فـلا توجد قوانين مشتركة ثنائية بين الدول حول البحث والتحقيق في هذه الجرائم وحول تسليم المجرمين ، وهذا ما يزيد الأمر تعقيداً وصعوبة. وهنالـك مشـاكل أخـرى مرتبطة بالقوانين نفسها، إذ تفتقر قوانين أصول المحاكمات الجزائية إلى النصوص القانونية اللازمة لمواجهة هذا النوع الجديد من الجرائم، فلا توجـد قواعـد تـنظم التفتيش في جرائم الحاسوب الحاصلة عبر الشبكات، كما أن هنالك غياباً للنصوص الإجرائية التي تتكفل بوضع ضوابط لتفتيش منظومات المعلومات واقتحامها(المناعسه واخرون ، 2001 ،(289 –294)) .

وتعد مسألة فهم الجوانب الفنية والتقنية التي تحيط بجرائم الحاسوب من أكثر الصعوبات التي تواجه المتخصصين في هذه الجرائم، من قضاء ونيابة عامة ورجال شرطة، نظراً لحداثة علم الحاسـوب والعلـوم المعلوماتيـة وأن أغلـب المفـاهيم المستخدمة لفهم طبيعة جرائم الحاسوب هي مفاهيم فنية وتقنية بحاجة إلـى وجـود خلفية ومعرفة سابقة بهذه المصطلحات مع ضرورة عقد دورات تدريبيـة، وكـذلك ضرورة ابتعاث العاملين في الجهاز القانوني لدراسة العلوم المعلوماتيـة الحديثـة، ورفد هذا الجهاز القانوني بعدد من أصحاب المعرفة والخبرة بهذا المجال. كما يؤدي أسلوب التبليغ عن جرائم الحاسوب دوراً كبيراً في عملية التحقيق وكشف الجريمـة عندما يكون التبليغ متكاملاً، إذ يجب أن يقدم التبليغ السـليم والمتكامـل الجوانـب والأطراف وصفاً علمياً محدداً للنشاط الإجرامي مع بيان الأسماء واللغات والبرامج وأنواع الأجهزة المستخدمة وأماكنها ، وعلى الأغلب يكون التبليغ ناقصاً وغير محدد بطريقة تساهم في عرقلة التحقيق وليس تسهيله، وذلك بسبب جهـل المبلـغ وعـدم إحاطته بكل جوانب الجريمة، وكذلك بسبب تدني الثقافة المعلوماتيـة لـدى عمـوم المجتمع . (البشري ، 1421هـ ،(355 – 365)).

وفيما يتعلق بأسباب ارتفاع أعداد الجرائم الحاسوبية غير المكتشفة، فهنالك أربعة أسباب واعتبارات تدل على ارتفاع عدد الجرائم غير المكتشفة في حقل المعلوماتية هي :- (رستم ، 2000 ، (90 – 92)) .

1-صعوبة كشف الجرائم التي ترتكب في مجال المعالجة الإلكترونية للبيانات وإثباتها .

2-حاجة هذه الجرائم إلى مواجهة فعاله وملاحقة قضائية لمرتكبيها تتطلب معرفة خاصة، وتستلزم بذل الكثير من الوقت والجهد والمال في التحري عنها والتحقيق فيها.

3- اكتفاء الجهات المجني عليها في أغلى الجرائم المعلوماتية المكتشفة باتخاذ إجراءات إدارية داخلية دون القيام بإجراء تبليغ عنها للسلطات المختصة خوفاً من الإضرار بسمعتها، وحدوث شرخ في ثقة المتعاملين معها سواء أكانوا أفراداً أم منظمات.

4-وجود غموض يكتنف مفهوم الجريمة المعلوماتية وجهل الناس بمفهومها وخطورتها، إذ تظهر الجرائم المعلوماتية التي تصل إلى علم السلطات في الإحصاءات ضمن جرائم الغش وإساءة الائتمان، لأنه ما يزال مصطلح الجريمة المرتكبة بوساطة الحاسوب غير مستخدم في الإحصاءات الرسمية، وما يزال هنالك قصور في إدراك هذه الجرائم .

أبرز إنجازات ومساهمات القانون في حماية الحاسوب

لابد من التأكيد أن موضوع جرائم الحاسوب هي في طور نموها على صعيد العالم بشكل عام والدول النامية بشكل خاص، فالدول العربية التي بادر بعضها بتطبيق الحكومة الإلكترونية هي من أكثر الدول تحركاً في اتجاه توفير حماية إلكترونية على صعيد الوطن العربي، إذ لا يمكن تحقيق نجاح للمعاملات الإلكترونية المختلفة سواء كانت معاملة تجارية إلكترونية أو حكومة الإلكترونية أو أي خدمات إلكترونية دون مساهمة التشريعات، وبخاصة الصارمة منها، في توفير حماية لهذه المعاملات، فقد كان من المفترض أن يقابل الثورة التي حصلت على صعيد

المعلوماتية ثوره أخرى على صعيد القوانين والتشريعات تساهم في التصدي للتهديدات التي تصيب الثروة الثمينة التي يحويها الحاسوب نفسه .

ومن أبرز التشريعات الصادرة لحماية المعاملات الإلكترونية على صعيد الوطن العربي القانون الصادر في تونس عام (2000) وهو قانون المبادلات التجارية الإلكترونية، وكذلك مشروع قانون التجارة الإلكترونية المصري، وقانون المعاملات الإلكترونية الأردني المؤقت رقم (85) لسنة (2001) والمادة (92) من قانون البنوك الأردني رقم (28) لسنة (2001) التي تتعلق بنظام المدفوعات ووسائل الإثبات الإلكتروني، والمادة(13) من قانون البيانات الأردني رقم(30) لسنة (1952) والمعدل بقانون رقم(37) لسنة (2001). (الصمادي ، 2003 ، (235 – 280)) .

هذا ليس حصراً لكل إنجازات القوانين المتصلة بنظم المعلومات، لكنه ذكر لبعض الإنجازات التي تساهم في توفير حماية للمعاملات الإلكترونية .

ففي المملكة الأردنية الهاشمية ساهم قانون الاتصالات رقم (13) لسنة (1995) في معالجة العديد من القضايا الخاصة بشبكات الاتصالات، كما دعم قانون حق المؤلف الأردني رقم (2) لسنة (1992) حماية العديد من الحقوق المرتبطة بالحاسوب وكذلك قانون الحماية الفكرية المعدل(صالح،2000،(10 – 12)) .

كما حدد المشرع الأردني تعريفاً لجريمة التزوير، وحدد أركانها في المواد (260،262،263) من قانون العقوبات الأردني، وعرفها على أنها "أي تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج به مما ينجم أو يمكن ان ينجم عنه ضرر مادي أو معنوي أو اجتماعي" وحدد ثلاثة أركان لجريمة التزوير هي :

1-ركن مادي، ويتمثل في تحريف مفتعل أو تغيير للحقيقة في محرر.

2-أن يترتب على التغيير ضرر مادي أو معنوي أو اجتماعي .

3-ركن معنوي، ويتمثل بالقصد الجرمي . (الدباس،2003،50) .

وحتى نواجه جرائم الحاسوب ، ونتصدى لها، ونحد منها، لابد من السير بخطوات متوازنة في الاتجاهين القانوني والمعلوماتي، كما أنه لابد من نشر وعي وثقافة تقنية بين أفراد المجتمع بشكل عام وفي صفوف رجال الأمن والقانون بشكل

خاص على اختلاف مجالاتهم، وتحديداً القضاة، وضباط العدليه، والمحققين، وذلك من خلال عقد دورات تدريبية وتثقيفية، بهدف توعيتهم بهذه النظم المعلوماتية ومحتوياتها، وكذلك لابد من السعي إلى إدخال علم تقنيات المعلومات إلى العلوم القانونية بحيث يصبح هنالك فرع مرتبط بالمعلوماتية وجرائم المعلوماتية يدرس في كليات الحقوق والقانون، وكذلك لابد من أن تكون التشريعات والقوانين الجزائية صارمة ورادعة حتى تردع الأفراد عن ارتكاب الجرائم وتحد من تزايدها .

نتائج التهديدات الأمنية

تتنوع نتائج التهديدات الأمنية، فمنها ما نلحظه ونتلمسه مباشرة فور حدوث التهديد مثل الأضرار التي تلحق (بماديات أنظمة المعلومات من أجهزه ومواقع ومحطات طرفية وطابعات وكذلك أضرار تمس الشبكات والتطبيقات وقواعد البيانات) أما النتائج غير المباشرة التي لا نلحظها فور وقوع التهديد ولا نستشعر بالضرر الذي لحق فيها مباشرة مثل (الموثوقية ، والخصوصية ، والتكاملية).

أولاً: النتائج المباشرة للتهديدات الأمنية

1- تهديد الأمن المادي

إن تعرض الأمن المادي لمراكز المعلومات للتهديد يعني فقدان عمل الأجهزة وملحقاتها، وتوقفها أو تلفها جزئياً أو كلياً، لكن تحقيق أمن مادي لمراكز المعلومات يتم من خلال إبقاء الأجهزة وملحقاتها عاملة دون توقف، وذلك بتوفير جميع الظروف المناسبة لعملها من رطوبة، ودرجة حرارة، ، وحسن اختيار موقع المركز مع الحرص على توفير الظروف المناسبة داخل مراكز المعلومات وخارجها بما يحقق أمنية لهذه المراكز ومحتوياتها من أجهزة ومعدات ومبانٍ وحتى الأفراد .

فتهديد الأمن المادي يعني إلحاق الضرر بالمنظمة كاملة من مبانٍ وغرف، وأجهزة، ووسائط معلومات، ومحطات طرفية، وأفراد. والضرر الذي يلحق بهذه الأجزاء المادية سهل الكشف والتلمس ومن أبرز الأخطار المادية التي يتعرض لها مركز الحاسوب في المنظمة (الحريق؛ وانقطاع التيار الكهربائي؛ والتعرض

لفيضانات؛ وانقطاع الاتصالات؛ والإهمال؛ والسرقة؛ والتخريب؛ والاقتحام). (داود، 2000، 36).

ويفترض إيجاد حماية مادية تتضمن التأكد من توفير وسائل وإجراءات الحماية لأجهزة الحاسوب، والشبكات، والبنى التحتية من وسائل الطاقة والتوصيلات، ومدى توافر وسائل الوقاية من الكوارث الطبيعية أو الحوادث المتعمدة إضافة إلى وسائل حماية مكان وجود الأجهزة والوسائط وأدلة الأمن المكتوبة والوسائل المادية للوصول إلى الأجهزة واستخدامها من المخولين.(عرب،2002 ، 187).

وتشتمل الحماية المادية على الوسائل كافة التي تمنع الوصول إلى نظم المعلومات وقواعدها من خلال الأقفال والحواجز والغرف المحصنة. (عرب ، 2002 ، 180) .

أنواع الحماية المادية

ولتحقيق حماية متكاملة لابد من الحرص على تأمين وحماية جميع أجزاء وأطراف الأمن المادي في المنظمة من مبانٍ، وغرف، وأجهزة، ومعدات، ووسائط، وأفراد .

أ- الحماية العامة للمباني

تعتبر عملية انتقاء موقع مبنى الحاسوب نقطة حساسة ومهمة لتحقيق حماية عامة للمبنى، إذ من الأهمية البالغة اختيار هذا الموقع بعيداً عن الأخطار البيئية المحتملة، وان يكون ذا تهوية جيدة مع ضرورة الحرص على تنظيم المرافق والخدمات داخل المبنى بشكل يضمن سلامته مثل الحرص على وضع خزانات المياه والوقود ودورات المياه في مواقع بعيدة عن غرف الحاسوب للوقاية من أضرارها في حالة حدوث ضرر أو تهديد عن طريقها. كما تجب الوقاية ضد الحريق من خلال استخدام المواد المقاومة للحريق، ومنع التدخين في مواقع العمل، والتعامل بحرص في تخزين المواد القابلة للاشتعال، واستخدام خزائن واقية ضد الحريق لوسائط تخزين البيانات، وتوفير معدات الإطفاء في كل موقع، واستخدام مفاتيح عازلة للأجهزة الكهربائية، واستخدام وسائل الكشف عن الحريق والإنذار بحدوثه مع ضرورة التأكد من سلامتها، وعمل صيانة لها بشكل دوري كما يجب استخدام مصدر يضمن استمرار الإمداد بالطاقة الكهربائية، واستخدام مولدات احتياطية لتوليد

الكهرباء، وكذلك العناية بالاتصالات الهاتفية وعمل صيانة مستمرة لها، واستخدام خطوط اتصال بديلة و تأمين خطوط الاتصال ضد التنصت والتخريب، والاهتمام بأجهزة تكييف الهواء بعمل صيانة مستمرة لوحدات التكيف والتبريد ومواسير المياه المستخدمة. (داود ، 2000 ، (37 –39)).

ب–تأمين الأجهزة داخل غرفة الحاسوب.

ويتحقق تأمين الأجهزة داخل غرف الحاسوب من خلال التقيد بمجموعه من الإجراءات:

1–ضبط إجراءات دخول وخروج أجهزة الحاسوب في المنظمة.

2–عدم السماح لموظفي الصيانة من خارج المنظمة بإدخال أو نزع البطاقات الإلكترونية، وكذلك ضرورة وجود مراقبة من داخل المنظمة لموظفي الصيانة الخارجين خوفاً من وضع أجهزة تنصت أو الإضرار بالأجهزة أو ما أشبه.

3–الحرص على تأمين احتياطي من الخدمات التي قد يسبب توقفها تلفاً للأجهزة أو تعطيل العمل مثل الطاقة الكهربائية، وتكييف الهواء مع ضرورة وجود خطة طوارئ في هذه الحالات وتدريب الموظفين على هذه الخطة وتطبيقاتها.(داود ، 2000 ،(46 –47)).

ج–تأمين النهايات الطرفية والطابعات . .(داود والمشهداني ،2001،63).

لابد من توافر حماية للنهايات الطرفية والطابعات نظراً للقيمة العالية للمخرجات التي تتم عن طريق الطابعات والاتصالات التي تحققها النهايات الطرفية. وأهم الإجراءات التي تحقق حماية وأمنية للنهايات الطرفية والطابعات :

1–متابعة سجل حركة الأعمال ودخول وخروج المستفيدين من والى النظام واستخدام المعلومات .

2–يجب عزل الطابعات ومطبوعاتها عن القاعة للحد من تعرف العاملين على محتويات المطبوعات التي غالباً ما تكون متضمنة معلومات سرية مع الحرص الشديد على ضرورة توفير مفاتيح لإغلاق الطرفيات أو الغرف التي تحتوي على الطرفيات في الأوقات التي لا يتم استخدامها فيه .

3- ضرورة التأكد من فصل الطابعات والطرفيات بعد انتهاء ساعات الدوام

د-أمن وسائط المعلومات

لا تقل أهمية آمن الوسائط التي تستخدم لتخزين المعلومات عن بقية عناصر الأمن المادي. ولتحقيق أمنية لهذه الوسائط لابد من :- .(داود ، 2000 ، (48 - 49))

1-توفير مستوى حماية مناسب للأسطوانات والأشرطة الممغنطة والأقراص الضوئية التي تحمل المعلومات .

2-الاهتمام بشؤون الوسائط التي تحتوي على النسخ الاحتياطية من الملفات، إذ يفضل الاحتفاظ بها في مكان بعيد عن الموقع، والحرص على استخدام وسائط تخزين في الموقع مقاومة ضد الحريق ومغلقة بإحكام مع ضرورة اقتصار الوصول إلى مناطق التخزين لهذه الوسائط على الأشخاص المصرح لهم .

3-يجب إتلاف النفايات والمخلفات مثل: البطاقات، وقوائم البرامج، والميكروفليم بشكل دوري من خلال استخدام أفران لحرق الأوراق والمخلفات .

4- كما يجب الحذر من الأجهزة الإلكترونية التي ينشأ عن استخدامها مجال مغناطيسي، وتحتوي على ملفات كهربائية لاحتمال تأثيرها على البيانات المسجلة.

5-ضرورة الحرص عند تخزين الوسائط القابلة للتفكيك والحمل مثل الأسطوانات المرنة والأشرطة بأن تتم عملية الفك في غرف مغلقة، ويكون هنالك إجراءات وسجلات تنظم تداولها.

ذ-أمن الأفراد

يعد الأفراد جزءاً مهماً من المنظمات وذا تأثير عظيم على الأمنية، ففي الوقت الذي يعتبر فيه الكادر الوظيفي من أثمن المصادر وأخطرها، فإن وعي هذا الكادر وحرصه على عمله والأجهزة التي يتعامل معها، وعلى سرية وخصوصية المعلومات هنا يعد من أثمن المصادر، وبمثابة خط الدفاع عن المنظمة لكن عدم المبالاة، وقلة وعي الكادر الوظيفي، وإقدامه على التخريب المقصود وغير المقصود للأجهزة والنظام، وإفشاء الأسرار، واختراق الخصوصية، تجعل الكادر الوظيفي من أخطر المصادر. وحتى نحقق حماية وأمنية مادية لما يتعامل معه الأفراد ينبغي تحديد الصلاحيات للعاملين، وضبط تحركاتهم، وتحديد المصرح وغير المصرح له

القيام بمهام العمل، وإقامة دورات توعية وتثقيف للأفراد القائمين على رأس عملهم. أما الأفراد الذين من المنتظر انضمامهم إلى الكادر الوظيفي، فتوضع ضوابط لاختيارهم، وتعيينهم والتأكد من سلوكياتهم وأخلاقياتهم مع ضرورة توافر خبرات عملية وعلميه في مجال العمل (داود والمشهداني ، 2001 (33 – 34))

2- تهديد أمن التطبيقات (البرامج)

تعد التطبيقات النصف الآخر المكمل للأجهزة وماديات الحاسوب، فالبرمجيات كالروح للجسد، وتحقيق أمنها وحمايتها لا يقل أهمية عن تحقيق لأمنية الجزء المادي من الحاسوب، إذ يهمنا تحقيق أمن لأنظمة التشغيل والبرامج المساعدة لها، والأنظمة العاملة على هذه الأجهزة. ويجب أن تحتوي هذه البرمجيات على وسائل تحدد عدد المستخدمين للنظام وصلاحياتهم. ويتضمن تحقيق أمن البرمجيات، على الأغلب، وجود أنظمة ضبط كلمات المرور والبرامج المضادة للفيروس، وتطبيقات حفظ البيانات والمعلومات، وتخزينها، واسترجاعها، بحيث تكون الإجراءات المستخدمة في ضبطها إجراءات صارمة وشديدة، نظراً لحساسية عملية النسخ الاحتياطي، فسلامة هذه العملية وتحقيق حماية لها يعني حماية البيانات والمعلومات التي تم تخزينها وسوف يتم استرجاعها عند الحاجة لها.(Cleary, 1998 ,206)

اختلاف بيئات العمل وأثره على أمن التطبيقات

وتكمن خطورة ومشكلة التطبيقات من الناحية الأمنية في بيئة العمل وتنوعها، ونظراً لأنه ليس من السهولة التشارك بشفافية بين بيئات عمل تستخدم نظم تشغيل مختلفة، فإن اختلاف بيئة العمل لها أثر على سهولة الحصول على الخدمة والوصول إلى قاعدة بيانات في نظام ما، إذ يستدعي اختلاف بيئة العمل تنظيم صلاحيات المستفيدين التي من الواجب التأكد منها قبل السماح لهم باستخدام التطبيقات. وهذه القضية تحتاج إلى تعاون نظام التشغيل لاتمام الوصول إلى قاعدة البيانات، مع الأخذ بالاعتبار أنه من الصعوبة بل من المستحيل إنتاج نظام تشغيل "سوبر" يستطيع التعامل مع جميع نظم التشغيل، ونظراً لهذه الحاجة الملحة نشأ مفهوم (الخادم، العميل) (Client Server) وهو جهاز كبير يخدم مجموعة من الأجهزة الأخرى الصغيرة، ويتمتع بالقدرة على تكوين الطلب وتوجيهه إلى الخادم المناسب بغض النظر عن نوع الخادم أو نظام تشغيله هذا في حالة وجود أكثر من خادم، وكل خادم

يجب ان يكون قادراً على تنفيذ كل مهمة بطريقة تناسب الطلب الموجه إليه، ولكن هنالك عدة مشاكل أمنية في بيئة (العميل /الخادم) أبرزها :-

1-قدرة تطبيقات العميل على أن تحدد احتياج طالب البيانات .

2-تقديم المعلومات الضرورية فقط دون غيرها.

3-تأمين المعلومات المستلمة بعد وصولها بالشكل المناسب .

4-قدرة التطبيق الموجود على جهاز العميل على تخزين البيانات المستلمة من الخادم، وتقديم مجموعة مكافئة من المهام للمستفيدين الذين يتعذر اتصالهم بجهاز الخادم، فعملية التخزين للبيانات على جهاز العميل لا تعتبر مشكلة لكن سرقة الحاسوب الدفتري (Note Book) من المستفيد مع ما يحتويه من معلومات مهمة هي المشكلة الحقيقية . (داود ، 2000 (253 – 255)).

تأمين التطبيقات

حتى نحقق جدار حماية وأمن للتطبيقات خوفاً من تسربها أو سرقتها أو تخريبها، لابد من الحرص على توفير أحزمة الأمان التالية :-

1-الأمن باستخدام القوائم بعد التحقق من شخصية المستفيد يتم تخزين صلاحياته بالنسبة لمختلف البيانات التي يحتويها الخادم وبمجرد طلب المستفيد لخدمة ما، فإنه يعرض له، حسب مستوى صلاحياته على شاشة الحاسوب مجموعة من القوائم، فيختار القائمة التي يريد الاستفادة منها فإذا كانت محتويات هذه القائمة ضمن صلاحيات المستفيد تفتح له وينسدل منها مجموعة من المهام، وإذا لم تكن ضمن صلاحياته، فإنها لا تفتح له، ولا تستجيب القائمة لطلبه. (داود، 2000، 295)

2- بناء كلمات المرور السرية بحيث لا يسمح لأي مستفيد استخدام الحاسوب. والتعامل مع البرمجيات المتوافرة إلا إذا كان صاحب صلاحيات، ويمتلك كلمة المرور. وهنا يجب الحرص على تغيير كلمات المرور بشكل مستمر، وعند محاولة المستفيد إدخال كلمة المرور السرية وحصول خطأ في الإدخال يجب رفض إعطائه تصريح الدخول إلا بعد التحقق من هويته ومن الجهة التي منحته كلمة السر، وإذا تكرر الخطأ يحرم من تلقي الخدمة.(داود والمشهداني، 2001، 93).

3-استخدام ملف التسجيل (Log File) يستخدم هذا الملف، بوصفه أحد وسائل الأمنية للحاسوب والبرمجيات، إذ يساعد على استرجاع السجلات المفقودة ومعالجتها، كما أنه يساهم في تحديد أسباب اعتبار السجلات غير سليمة، ويتابع تاريخ إدخال السجلات، ويحدد مصادر المعلومات المضللة المرسلة إلى الحاسوب، ويصحح الملفات ذات البرامج الخاطئة المؤدية إلى تلف بعض البيانات، ويساهم في كشف التلاعب بمحتويات الملفات وتسجيل الملفات المراد تحديثها.(داود والمشهداني، 2001، 95).

3-تهديد أمن قواعد البيانات

تمتاز عملية تحقيق الأمنية لأنظمة المعلومات بأنها عملية مترابطة ومتكاملة، فبعد تحقيق الأمنية المادية ومن بعدها أمنية التطبيقات نأتي إلى أمنية قواعد البيانات.

قواعد البيانات (Database) "هي مجموعه متكاملة من البيانات التي تم تنظيمها على الصورة التي تمكن العديد من المستفيدين في المنظمة من التعامل معها" وتسهيلاً على المستفيدين في التعامل مع قواعد البيانات؛ فإنهم يستخدمون لغات للاستفسار و المعالجة مثل لغة (SQL) Structured Query Language أما المختصون، فيعتمدون على نظم إدارة البيانات (DBMS) لإدارة ومعالجة وتأمين قواعد البيانات (داود ، 2000، 296) .

ويكمن السبب في تزايد أهمية قواعد البيانات وتعاظم خطورة تعرضها لتهديد في احتواء قواعد البيانات على تجمع الكثير من البيانات الخاصة بالمنظمة في قاعدة أو أكثر من قواعد البيانات مما يساهم في تفادي تكرار عديد من البيانات، وتفادي المشكلات الناجمة عن تحديث بعض الملفات وعدم تحديث البعض الآخر. وعليه، فان وجود المعلومات في إناء واحد يجعل عملية الضبط والتحكم والرقابة للمعلومات وتأمينها أمراً أكثر سهولة. ولتحقيق حماية وأمن متكامل لقواعد البيانات لابد من معرفة وتحديد الفئات التي تستخدم هذه القواعد، وهي: (المستفيدون، والمبرمجون، المشغلون، ومدير قاعدة البيانات، ومسؤول أمن قواعد البيانات) مع ملاحظة ان اغلب المستخدمين لقواعد البيانات هم من المتخصصين وأصحاب الخبرة في

البرمجة والتشغيل. لذلك لابد من الحرص في التعامل معهم بالإضافة إلى تحديد صلاحياتهم ومراقبتهم باستمرار.(داود ، 2001 ، (270 – 271)) .

أشهر نماذج قواعد البيانات

حتى نتمكن من تحديد أساليب الحماية لقواعد البيانات، لا بد لنا من التعرف، ولو على جانب من أنواع قواعد البيانات وسوف نستعرض اشهر ثلاثة أنواع وأكثرها تداولاً في المنظمات وهي :-

أ_قواعد البيانات الهرمية، وتناسب البيانات التي تتفق طبيعتها والطبيعة الهرمية، فتكون العلاقة بين البيانات إما مفردة أو متعددة، ويؤخذ على هذا النموذج أنه بطيء ويكرر البيانات .

ب- قواعد البيانات الشبكية، وتناسب البيانات التي تتشابك فيها العلاقات بين العناصر، إذ يتم تمثيل البيانات كمجموعات من السجلات والعلاقة المختلفة بين هذه السجلات، لكن يؤخذ على هذا النموذج أنه معقد وصعب الاستخدام كما أنه لا يناسب كل لغات أجيال الحاسوب، فهو يناسب لغات الجيل الثالث .

ج- قواعد البيانات العلاقيه، ويتم تنظيم المعلومات على شكل جداول مكونه من صفوف وأعمدة تربط كل عامود وصف علاقة، ويمكن إيجاد علاقة بين عدة جداول والربط بينها، ويعتبر أفضل الأنواع وأكثرها مرونة وفاعلية بين أنواع ونماذج القواعد، لأن صورة الجدول هي أبسط صوره تنظم البيانات، وأكثرها منطقية، وأقربها إلى الفهم، كما يتصف بالجاذبية، لأنه يناسب معظم أنواع البيانات بالإضافة إلى مناسبته للغات البرمجة الحديثة. (داود ، 2000 ،(275 –276))

خطة تأمين البيانات.

من الأفضل لتحقيق حماية متكاملة لقواعد البيانات القيام بعمل خطة تأمين للبيانات تهدف إلى الوقاية من التهديدات قبل وقوعها وفي الوقت نفسه علاج ما وقع من تهديدات، وذلك من خلال تأمين البيانات وحمايتها من الفقدان أو التلف أو سوء الاستخدام في حال فشل إجراءات تأمينها .

وأهم مرحلة في خطة التأمين هي تحديد الموارد المراد حمايتها، وأهم هذه الموارد (البيانات التي تحتويها الجداول، وهياكل البيانات، وبرامج معالجة البيانات، وإجراءات نسخ البيانات واسترجاعها، وكذلك الوسائط التي تحتوي على بيانات مثل الأقراص الممغنطة، وتنفيذ البرامج، وإجراءاتها، والطرفيات) فبعد تحديد الموارد المراد حمايتها، لابد من تحديد ما هي الأساليب المناسبة لتأمين هذه الموارد، وهذه الأساليب تختلف من منظمة إلى أخرى، ومن مورد إلى آخر.(داود ، 2000 ،(277 – 278)) .

وسائل أمن البيانات في النموذج العلاقي

كون النموذج العلاقي أهم نماذج قواعد البيانات واكثرها مرونة و أوسعها انتشاراً في أغلب المنظمات، فسوف نتناول أهم وسائل تأمين البيانات في قواعد البيانات العلاقيه، وأهم هذه الوسائل :_

1-سلامة العناصر وتكاملها، ويتم تحقيقه عن طريق تأمين المفتاح الرئيسي للجدول، وضمان صحته، ويشترط أن يكون المفتاح الرئيسي للجدول منفرداً وغير متكــرر، وأن يكون هنالك قيمة محددة للمفتاح الرئيسي للجدول .

2-السلامة الرجعية، وهي من أكثر المبادئ أهمية لتحقيق سلامة البيانات وصحتها وتكاملها، إذ يشترط لتحقيق السلامة الرجعية في حالة اعتماد جدول ما على جــدول آخر (أي حين تعتمد قيم أحد أعمدة هذا الجدول على المفتاح الرئيسي لجدول آخر) أن تكون القيم الواردة في هذا العمود مساوية لأحد قيم المفتاح الرئيسي في الجـــدول الآخر، وتطلق تسمية(الجدول المشير)على الجدول الذي يعتمد على جدول آخر.

3-حجز البيانات : وهو أسلوب يستخدم لتأمين البيانات في قواعد البيانات، إذ يــتم حجز البيانات التي يجري تعديلها بوساطة أحد المستفيدين حتى يتم التعديل ثم تتـــاح البيانات بعد ذلك لأي مستفيد آخر، وهنالك شكلان للحجر هما: الحجر المحدود الذي يسمح للمستفيدين الآخرين بقراءة البيانات فقط دون أن يكون لهم الحق في تعديلها، والحجر المطلق والذي لا يسمح فيه لأي مستفيد باستخدام البيانـــات لا للقــراءة ولا للتعديل .

4-المنظورات، ويستخدم المنظور بوصفه وسيلة فعالة لتأمين البيانات، ويتم بوساطته تحديد نافذة للمستفيد يرى من خلالها ما يهمه من قاعدة البيانات، فلا يرى الجدول كاملاً، ولكن يرى ما يهمه من صفوف وأعمدة من هذا الجدول فقط .

5-توزيع الصلاحيات على المستفيدين، وذلك بتنظيم تداول البيانات واستخدامها، إذ يتم حفظ توزيع هذه الصلاحيات في نظام إدارة قواعد البيانات في قاموس البيانات أو في جداول النظام، وعند أي طلب باستخدام البيانات من جانب المستفيدين يتم الرجوع إلى هذه الجداول وهذا القاموس لمعرفة ما هو مستوى صلاحياته، ويعمل إلى جانب نظام إدارة قواعد البيانات نظام الاتصالات المباشر، ونظام التشغيل، ونظام أمن البيانات، ولضمان نجاح عمل هذه الأنظمة وعملها بتناغم وتفادي أي تكرار أو تعارض بين بعضها البعض، لابد من إعطاء كل مستفيد رقم استخدام واحداً ينفذ بوساطته إلى البيانات، ولا يستخدم المستفيد في النظام سوى هذا الرقم، ويحدد لهذا الرقم الصلاحيات المناسبة في كل مراحل التعامل مع البيانات . (داود ، 2000 ،(279 -286)) .

4 -تهديد أمن الشبكات

لا يعني عمل الحاسوب الشخصي بشكل منفرد دون ارتباطه مع حواسيب أخرى عناءً و هاجساً وتهديداً كما هو عند ارتباط الحواسيب مع بعضها البعض لتشكل شبكات، إذ تعني الشبكات عدد حواسيب أكبر ومستخدمين بأعداد هائلة في تزايد مستمر سواء كانت الشبكات محلية (إنترانت) أو عالمية (إنترنت) فالخطر والتهديد في تزايد وليس بالهين، وعواقب الاستهانة والاستخفاف بحجم الضرر الشامل لكل أجزاء نظم المعلومات ليست بسيطة .

فالاتصال بالإنترنت وإرسال معلومات بوساطة الشبكات الداخلية والخارجية يتطلب إجراءات أمن خاصة. وتعتبر شبكات العمل العامة الكبرى متضمنة الإنترنت عرضة للهجوم بشكل أكبر، لأنها مفتوحة فعلياً وعملياً لأي شخص. ونظراً لاتساع هذه الشبكات فإن تعرضها للتهديد وإلحاق الضرر بها يكون له تأثير هائل وحجم الضرر المتحقق كبيراً، وعملية ربط الحواسيب بالشبكة العالمية الإنترنت بشكل مستمر يجعلها مفتوحة للاختراق من قبل الأشخاص الخارجيين، لأنهم يستخدمون عنوان إنترنت ثابت والذي يمكن تجديده ببساطة من خلال خدمة الاتصال. لذا يتم

تخصيص عنوان إنترنت مؤقت لكل سلسله أو دوره، لأن عنوان الإنترنت الثابت يخلق هدفاً ثابتاً للمقتحمين. (Laudon & Landon, 2002, 445) .

ويتضمن أمن الشبكات " مجموعة الإجراءات والقوانين والأنظمة التي يتم مزجها بهدف تأمين حماية وتكامل وجاهزية كل من المعلومات والوسائط والأجهزة المستخدمة في خطوط معالجة وتبادل هذه المعلومات عبر الشبكة "(داود ، 2000 ، 151)

وتحقيق أمن الشبكات أمراً في غاية التعقيد والتشابك لانه يشتمل على أجزاء عدة (الحواسيب المرتبطة بالشبكة ومعدات الاتصال، والتراسل، والكوابل، والأجهزة الملحقة بالحاسوب مثل: الطابعات، والشاشات، وأقراص التخزين، والبرمجيات) فكون الأجزاء المطلوب حمايتها لتحقيق أمن الشبكات متنوعة، فالأخطار التي تلحق هذه الأجزاء متنوعة أيضاً ومن أبرز الأخطار التي تهدد الشبكات وأهم آثارها.

ا- تعطل النهاية الطرفية (Terminal) وحصول أعطال في الخطوط وأجهزة "المودم" (Modems) يؤدي إلى انقطاع الخدمة وتلف البيانات.

ب- السرقة أو التدمير ومهاجمة الخطوط ومراكز الاتصالات وتعطل بعض الأجهزة أو وسيلة نقل البيانات تؤدي إلى انقطاع الخدمة.

ج-الاستخدام غير المصرح به للطرفيات ويؤدي إلى تلف البيانات، وإفشاء بيانات سرية وسرقة المعلومات.

د-حصول غير المصرح لهم على المعلومات يؤدي إلى إفشاء بيانات عن الأشخاص أو عن العمل.

ذ-التشويش على الإشارات المنقولة يؤدي إلى انقطاع الخدمة وتشويه البيانات.

هـ الاقتحام يؤدي إلى حصول غير المرخص لهم على البيانات السرية.

و-أعطال البرمجيات تؤدي إلى انقطاع الخدمة وعدم الثقة في سلامة البيانات.

ي-أخطاء التشغيل تؤدي إلى عدم الثقة في سلامة النظام بمجمله(داود،2000 ،(08 3-09 3))

أهم وسائل تأمين المعلومات في الشبكات المحلية

1-دور برامج التشغيل في الشبكة، ويتبلور هذا الدور في أنها تجعل المرافق البعيدة عن الحاسوب من الطابعات والملفات المخزنة على الأقراص الصلبة تبدو كمرافق

محلية، ولذلك تؤدي نظم التشغيل دوراً أساسياً في تحقيق سلامة البيانات والشبكات وذلك من خلال أعداد النسخ الاحتياطية للبيانات، وتمييز المستخدم، وتحديد صلاحياته من خلال كلمات المرور والقيام بتحديد صلاحيات استخدام الملف مثل: (الحذف؛ والإنشاء؛ والقراءة فقط؛ قراءة؛ والتعديل) واستخدام برامج تشخيص الأخطاء وبرامج تـدقيق القـراءة بعـد الكتابة للتأكد من أن ما تم كتابته من البيانات مطابق للبيانات الأصلية.

2-اختيار أنظمة التشغيل لابد من الحرص واليقظة عند اختيـار نظـام التشـغيل المناسب للشبكة، والتأكد من العوامل الفنية التالية :

أ- الحد الأقصى المتوقع من الحاسبات الشخصية المستضافة.

ب- هل تستدعي الحاجة إلى خلط اكثر من نوع من الحاسب مـن طـرز مختلفـة ضمن الشبكة.

ج-هل تستدعي الحاجة إلى خلط الحاسبات تستخدم نظم تشغيل مختلفة.

د- هل تستدعي الحاجة إلى ربط الشبكة المحلية عبر خطوط الهاتف مـع شـبكات أخرى أو حاسبات بعيده .

3-دور البرامج المساندة لنظم التشغيل في تأمين الشبكات المحلية، إذ تـؤدي هـذه البرامج دور المعاون للمستخدمين، فهذه البرامج الخاصة متضمنة في نظام التشغيل، وتقوم بإنجاز مهام معينة للمستخدم، ومن هذه البرامج :-

أ-البرامج المساندة لإدارة خادم الملفات، وتساعد هذه البرامج المستخدم في استخدام القرص الصلب في خادم الملفات وتمكينه من بناء الفهارس المنطقية على القرص .

ب-البرامج المساندة لإدارة الطباعة، وتتيح للمستخدمين فرصة التشارك في الطباعة على طابعة مشتركة في الوقت الواحد، وإذا كانت الطابعة مشـغولة فيـتم وضـع البيانات المطلوب طباعتها في طابور الانتظار إلى حين انتهاء الطابعة من الطباعة.

ج-البرامج المساندة للدخول، يقوم بمعالجة إجراءات الدخول إلى بيئـة الشـبكة، إذ توفر حماية للبيانات من الاستخدام غير المخول من خلال اسم وكلمة المرور.

د-البرامج المساندة للفهارس، وتهدف لحماية الفهارس من خلال جعل الصـلاحيات للملفات وليس للمستفيد .

ذ-البرامج المساندة للإغلاق، وتتولى هذه البرامج خطر استخدام الملف أو السجل أو الحقل لصالح فرد معين دون غيره حتى ينتهي من عمله .

4-الوسائل المادية لتأمين الشبكات المحلية، و تتنوع الوسائل المادية المستخدمة لتحقيق حماية الشبكات المحلية وتأمينها. ومن أبرز هذه الوسائل :-

أ-الأقفال الإلكترونية.

ب- أقفال الحاسبات الشخصية الحديثة، إذ تسمح للمحطة الطرفية بالبقاء على خط ضمن الشبكة حتى لا تتعطل الشبكة .

ج- نظم الإنذار الآلية، وتركب على الأبواب والنوافذ وتدق للتنبيه عن محاولات الاستخدام غير المرخصة في غير مواعيد العمل .

د-إلغاء وحدات إدارة الأقراص المرنة بهدف التغلب على المحاولات غير المشروعة لاستنساخ البيانات .

ذ-الحماية ضد الإشعاع الثانوي للكابلات من خلال وضعها في أماكن محمية غير معرضة لوصول غير المختصين، واستخدام الكابل المغلف وكابلات الألياف الضوئية التي تساهم في إلغاء عملية الإشعاع الثانوي للكوابل .أمن الشبكات العالمية (الانترنت) .

تزداد خطورة مشكلة الأمن وحدتها في الشبكات خصوصاً في الشبكات العالمية بسبب تزايد عدد الأجهزة المرتبطة عبر الشبكة، وتزايد عدد المستخدمين، وكذلك استخدامات وخدمات الشبكة عبر الإنترنت من (خدمات الحكومة الإلكترونية، والمحادثة، والتجارة الإلكترونية، والبريد الإلكتروني، ومقهى الإنترنت) وغير الكثير من الخدمات. وساهم الاتساع المتسارع في حجم الشبكة وفي عدد مستخدميها في تزايد مصادر التهديدات، وتزايد الموارد المعرضة للتهديد. وعليه، سوف يزداد القلق الذي يكتنف المهتمين بالأمنية، وعلى الأغلب تعد قضية الأمنية الهم الأكبر والشغل الشاغل على صعيد عالم المعلوماتية، فلابد للشركات والمنظمات والمؤسسات المسؤولة عن الأمنية من العمل بخطوات سريعة ومتواصلة حتى يتصدوا للتهديدات أولاً بأول. (داود ،2000 ،(325 - 332))

أهم وسائل الحماية في الشبكة العالمية الإنترنت

كثيرة هي الوسائل المستخدمة لحماية الشبكة العالمية، لكن أكثرها أهمية وفاعلية وشيوعاً على صعيد أمنية الشبكات في المنظمات هو جدار الحماية "جدار النار (Fire Wall") .

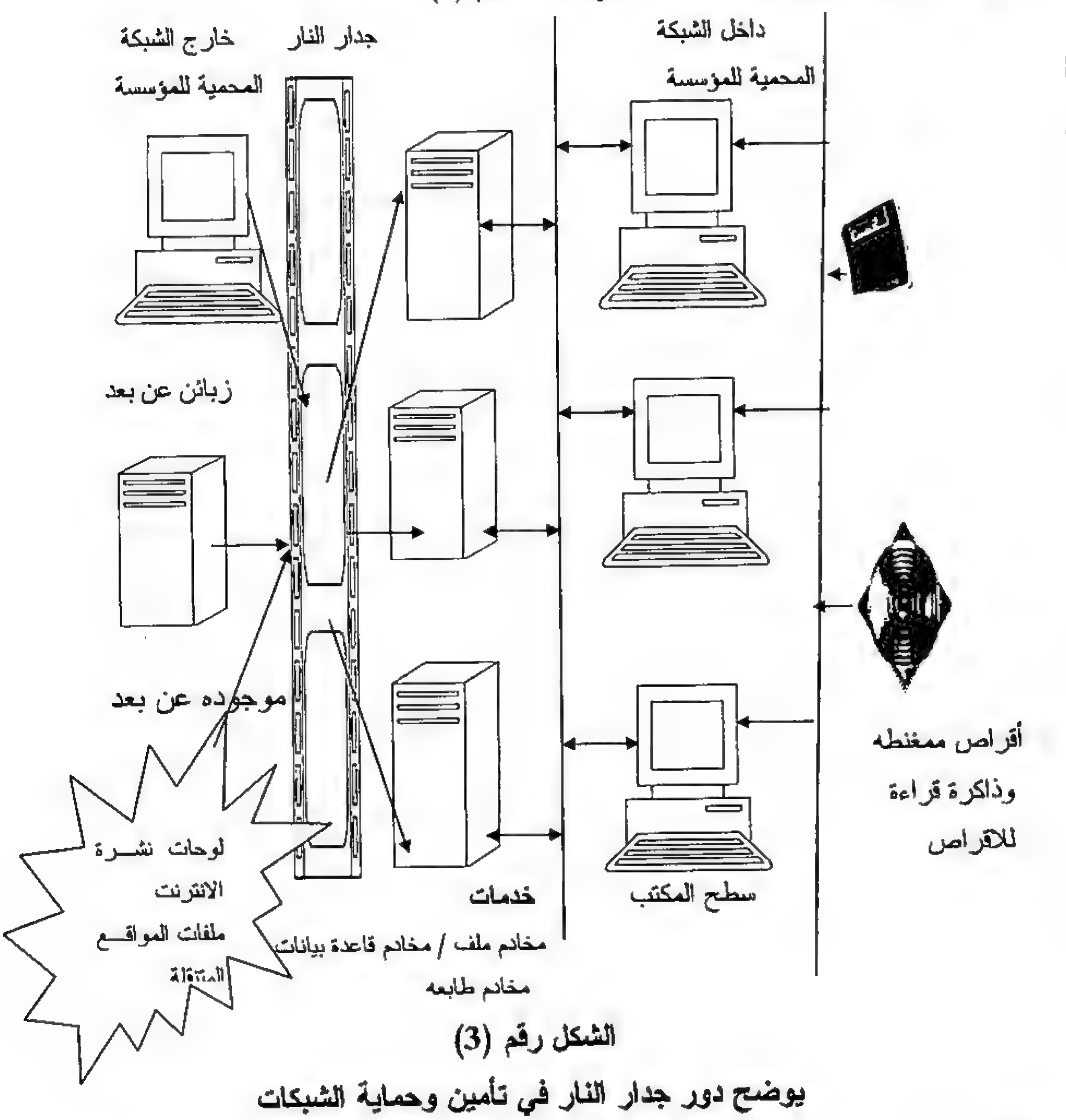
تستخدم جدران النار (الحماية) بوصفه وسيلة أو سياسة أمنية تمنع الوصول غير الشرعي للشبكات، وبخاصة من جانب المستخدمين . فمع تزايد المنظمات التي تعرضت شبكاتها للاختراق والقرصنة والتهديد، أصبحت جدران النار ضرورية ومن متطلبات الحماية والأمنية للشبكة. وتتمركز جدران الحماية، بشكل عام، بين الشبكات الداخلية والخارجية مثل (الإنترنت) إذ تقوم جدران الحماية بضبط عملية الوصول إلى الشبكات الداخلية لنظام المنظمة عن طريق قيامها بدور حامي البوابة الذي يفحص أوراق اعتماد كل مستخدم قبل السماح له بالوصول إلى الشبكة، وتحدد هذه الجدران الأسماء والعناوين للبرتوكولات الإنترنت (البروتوكول هو مجموعة متسلسلة من الإجراءات المتفق عليها من الأفعال لتنفيذ وظيفة ما) كما تحدد التطبيقات وسمات ومميزات حركة التجارة الإلكترونية ، فهي تفحص هذه المعلومات ضد طرق الوصول غير المشروعة التي تتم برمجتها للنظام عن طريق مدير الشبكة، كما تساهم بمنع الاتصال غير الشرعي إلى داخل الشبكة وخارجها، وتسمح للمنظمة بالقيام بتعزيز سياسة أمنية للحركة التي تجري بين شبكاتها والإنترنت .

وترتكز تكنولوجيا جدران الحماية على نوعين أساسين هما:-

أ-التفويضات، وتقوم بتوقيف البيانات من النشوء خارج المنظمة في جدران الحماية، وفحصها، وتمرير التفويض إلى الجانب الآخر من جدار الحماية . وإذا أراد مستخدم من خارج المنظمة الاتصال بمستخدم من داخل المنظمة، فإن المستخدم الخارجي يقوم أولاً بالحديث مع تطبيق التفويض الذي يتصل مع حاسوب المنظمة الداخلي، وبطريقة مماثلة يقوم مستخدم الحاسوب داخل المنظمة بالمرور خلال التفويض للتكلم مع الحواسيب الخارجية، وتعتبر التفويضات أكثر أمناً من المرتكز الآخر(الفحص النظامي) لانه في حالة الفحص النظامي لا تمر الرسالة الفعلية خلال جدار الحماية .

ب-الفحص النظامي، ويتولى جدار الحماية فحص كل مجموعة من البيانات القادمة ومصدرها، والعناوين المخصصة أو الخدمات، ويقوم بإنشاء جداول نظامية لتتبع المعلومات وفق مجموعات متعددة، ولابد من أن تحدد طرق وصول المستخدم إلى كل نوع من المجموعة التي لا تريد المنظمة قبولها، و يستهلك الفحص النظامي من مصادر الشبكة أكثر من التفويض أثناء أداء عمله. ((laudon& laudon, 2002, (446 – 447)

وتستطيع جدران الحماية إعاقة عملية اختراق الشبكة من الأشخاص الخارجيين، لكنها لا تمنعها بشكل كامل، ويجب اعتبارها عنصراً واحداً أو جزءاً في خطة الأمن الشاملة. ويتطلب تحقيق أمن الشبكات العالمية الاعتماد على سياسات مشتركة واسعة، وإجراءات أكثر حدة وصرامة ضد من يقوم بالتهديدات والاختراقات، بالإضافة إلى أهمية نشر الوعي الأمني على صعيد المنظمات بشكل خاص وعلى الصعيد الخارجي بشكل عام وفيما يلي توضيح لهذه السياسة الأمنية في الشكل رقم (3):



الشكل رقم (3)

يوضح دور جدار النار في تأمين وحماية الشبكات

المصـــــدر : (Alter, Steven,(1999), information systems ,Addison-Wesley Educational,Publishers Inc , p481)

ثانياً :النتائج غير المباشرة للتهديدات الأمنية

هي الجزء الثاني من النتائج التي تنجم عن مسببات التهديدات(مصـــادره) وتشتمل النتائج غير المباشرة على(الموثوقية؛ والخصوصـــية؛ والتكامليـــة "ســـلامة المحتوى" وتعد هذه النتائج المترتبة على حدوث التهديد التي لا نلحظها ولا نشعر بها فور حصول التهديد نتائج غير مباشرة، ولا يقل خطر تعرض هـــذه النتـــائج إلـــى التهديد عن خطر تعرض النتائج المباشرة للتهديد .

ولكل منظمة بما فيها المنظمات الحكومية معلوماتها الخاصة بها التـــي تعتبرها أسراراً يجب حمايتها مثل: الأبحاث، والتصاميم، والعمليـــات الصـــناعية، وتسويق المعلومات المهمة، والاستراتيجيات وغيرها الكثير من المعلومات المهمـــة والحساسة. وهذه المعلومات مهمة وضرورية للاستفادة منها لصالح المنظمة، وهـــذا يدعو إلى حمايتها فقد يعني عدم القدرة على استخدامها بصورة موثوقيـــة حصـــول شرخ في الثقة بين المنظمة والمنظمات الأخرى من جهة، وما بينها وبين العـــاملين والمتعاملين معها من جهة أخرى، ومن ثم فقدان الثقة. والأخطر من ذلك أن المنظمة قد لا تدرك أبداً السبب الكامن وراء الاعتداء علـــى أعمالهـــا، فلربمـــا تتعـــرض المعلومات غير المحمية للاختراق والخطر دون ترك أثر أو دليل على هذا الاختراق وهنا المشكلة الأكبر والأكثر تعقيداً. وحتى نضمن حماية المعلومات. هنالك ثلاثـــة أهداف أمنية، والبعض يعتبرها مبادئ رئيسية لسياسة الحماية هي: (Kevin , 1997, 3).

أ-السرية : حماية المعلومات من التعرض للكشف غير المرخص.

ب-التكامل : حماية المعلومات من التعديل غير المرخص .

ج-الموجودية:ضمان وجود المعلومات في وقت الحاجة لها.

وكثيرة هي الكتب والمقالات التي تحدثت عن هذه النتائج مع وجود تنـــوع فيها بحيث تزيد أو تنقص، فمنهم من حددها بالخصوصية والسرية والتكاملية ومنهم من اقتصرها على الموجودية، والموثوقية، ومنهم من أضاف إليها سلامة المحتوى. ومهما تنوعت فهي في محورها تدور حول مواضيع واحدة ذات محتوى متقارب.

وعندما يتعرض الحاسوب إلى هجوم أو تهديد؛ فإن ما يتعرض للخطر ليس الحاسوب كجهاز فقط بل يتعدى ذلك إلى البرمجيات، والشبكات، وقواعد البيانـــات،

وما تحتويه من بيانات ومعلومات مهمة وحساسة خاصة بالمنظمة. ويشكل الاطلاع عليها مشكلة، فكيف إذا تم عقب الاطلاع عليها النشر والتحريف والتعديل لهذه المعلومات. هذا على صعيد المنظمة، لكن ماذا عن الحكومة الإلكترونية التي تجمع وتحتفظ وتخزن كماً هائلاً من المعلومات عن حياة مواطنيها، بعضها معلومات خطيرة وحساسة ، فلا بد من أن تكون الحكومة جاهزة ومستعدة ومسؤولة عن حماية هذا الكم الهائل، خاصة ونحن بصدد التحول نحو الحكومة الإلكترونية . فينبغي قبل جمع المعلومات الشخصية المالية والمدنية والطبية الحساسة للحكومة من بناء سياسة حماية متينة وواسعة بقدر اتساع الشبكات، وتزايد عدد مستخدميها، وتزايد حجم التهديدات مع ضرورة بناء جسور الثقة بين الحكومة والمواطن والمنظمات التجارية، وذلك من خلال حرص الحكومة على توفير خصوصية هذه الأطراف، والمحافظة على أسرارهم بحيث لا يستهان ولا يسمح لأحد بالاطلاع عليها، أو تحريفها على اعتبار أن هذا حق من الحقوق التي منحها الله لعباده، وأقرها في كتابة الكريم والآيات الكريمة التالية تؤكد ذلك:

﴿ يا أيها الذين آمنوا لا تدخلوا بيوتا غير بيوتكم حتى تستأنسوا وتسلموا على أهلها﴾ (النور،آية27)

﴿ ولا تجسسوا ولا يغتب بعضكم بعضاً ﴾ (الحجرات،آية12)

وتؤكد هذه الآيات الكريمة على حق أعطاه الله لعباده، وهو حق الخصوصية في المسكن، وحرمة هذا المسكن التي لا تعطي أحداً الأحقية في هذه الخصوصية إلا بإذن صاحب المسكن، وكذلك تؤكد الآية الكريمة الثانية على رفض التجسس وخطره، ورفض الاستغابة بذكر خصوصيات الفرد للعامة. إذاً فالحاجة عندنا ليست إلى منظمات تعترف بحق الخصوصية، لأنه حق معترف به من الله عز وجل، ولكن الحاجة هي إلى منظمات تنظم هذا الحق وتراقب سيره

أهم النتائج غير المباشرة للتهديدات الأمنية

1-تهديد الموثوقية

لقد برزت الموثوقية(Authentication) على صعيد أنظمة المعلومات باعتبارها واحدة من أهم المواضيع المثيرة للاهتمام في القرن الحادي والعشرين، وترتكز الموثوقية على ثلاثة أبعاد هي: (Marjorys , 1999 ,1) .

أ-أمن المعلومات ب-خصوصية البيانات الشخصية ج-سلامة النظام.

والموثوقية هي العملية التي يتحقق بمقتضاها مدى أصالة المعلومات المتوافرة ومصداقيتها، وتكاملها، وخلوها من أي إفساد أو تزييف مع ضرورة الحرص على التأكد من مصداقية الأشخاص والعمليات بوساطة طرق التحقق من المصداقية، وهي:

أ-الصفات الشخصية مثل: المظهر؛ والصوت؛ والخط .

ب-سر من الأسرار مثل: كلمات المرور؛ ومفاتيح فك الشيفره؛ أو أرقام التحقق الشخصية.

ج-حيازة شئ معين مثل: البطاقة الشخصية، أو كرت الدخول .

د-الموقع أو المعلومة.

وكثيراً ما يتم استخدام أكثر من طريقه في الوقت نفسه للتحقق من الموثوقية، وذلك لزيادة هذه الموثوقية.(بداينة، 2002، 373) .

ولا يعني استخدام مصطلح السرية الموثوقية أن هناك تعارضاً أو اختلافاً في جوهر المضمون، لكن المصطلحين مترادفان، فحماية الأسرار يزيد من الموثوقية. وتوافر الموثوقية يعني حماية الأسرار .

فالسرية تعني حصر المعلومات في إطار عدد محدد من الأشخاص من خلال حمايتها ضد التعرض للكشف غير المشروع وغير المرخص، فالمحافظة على السرية للمعلومات تتوقف على سهولة أو عدم سهولة اختراق نظام الأمن والحماية وعلى حرية البيانات، وإتاحتها، وتداولها .(حجازي ،2002 ، 282) .

ولابد من السعي إلى تحقيق السرية والموثوقية للمعلومات التي تقود إلى بناء الثقة، وتعد من أهم متطلبات نجاح أي مشروع في كل مراحله، وهذا ما تسعى الحكومة الإلكترونية إلى تحقيقه من خلال بناء جسور اتصالات مفتوحة بين العاملين والإدارة، وتعتمد على استراتيجيات الشفافية، إذ تساهم هذه الشفافية في فهم المواطن للكيفية التي تتخذها الحكومة في إصدار قراراتها وفي عملها؛ ويساهم اطلاعه عليها في تفادي الرغبة في الاختراق، والتعرف على المعلومات، وينبغي توعية الموظفين إلى أن المعلومات الموجودة لديهم الخاصة بالمواطنين، والمعلومات المتعلقة بالعمل

وأسراره هي أمانة بين أيديهم وهم مسؤولون عنها، ويجب عدم إفشائها أو تعديلها. (LANVIN,2002 , 17) .

وتحقيق السرية يستدعي (منع أي شخص غير مخول بالنفاذ إلى معلومات النظام، واستخدام تلك المعلومات، وكذلك السيطرة على وصول الأشخاص المخولين إلى مستوى معين من تلك المعلومات، ومنعهم من الوصول إلى مستويات أخرى من المعلومات غير المرخص لهم الوصول إليها).(داود والمشهداني ، 2001 ، 20) .

وأكبر دليل على الاهتمام بموضوع الموثوقية هو استخدام الولايات المتحدة الأمريكية لمعيار تقييم الموثوقية لحماية أمن الحاسوب " T C S E C " (Trusted Computer Security Evaluation Criteria) وهذا المعيار يستخدم لتقييم الأنظمة والمشتريات التي تستجلبها الحكومة. أما على صعيد أوروبا؛ فيجري تطبيق التقييم طبقاً ل (I T S E C) (Information Technology Security Evaluation Criteria) وهو معيار الحماية الخاص بتكنولوجيا المعلومات ويستخدم هذا المعيار في كل من بريطانيا، وفرنسا، وألمانيا مضافاً إليـــــه مجموعة من المعايير المحلية حسب كل بلد (Kevin , 1997 ,5) .

الموثوقية والقانون (منصور،2002،(269 –271)) .

أما عن دور القانون في إقرار الموثوقية وحمايتها وتنظيمها والمحافظة عليها، فيتجلى بإقرار القانون حماية سرية وحرمة المراسلات والاتصالات الهاتفية، إذ لا تجوز مراقبتها أو إفشاء سريتها، إلا في الحالات المبينة في القانون ،ويجب على المرسل إليه احترام الأسرار الخاصة والعائلية التي تتضمنها الرسالة، سواء ما كان يتعلق منها بالمرسل أو غيره، وليس هنالك حق للمرسل إليه في تقديم رسالة سرية للقضاء، إلا إذا أذن له المرسل وعلى من يطلع على الأسرار بحكم وظيفته أن يمتنع عن إفشاء الأسرار حتى لو انتهى عمله، ولا يجوز لأحد الزوجين ان يفشي أسرار الزوجية بغير رضا الآخر حتى بعد الانفصال، إلا في حالة رفع دعوى من أحدهما على الآخر، كما يمنع القانون أصحاب المهن إفشاء الأسرار التي يؤتمنون عليها، ويعتبر إفشاء أسرار العمل جريمة يعاقب عليها جنائياً، ويجوز للمعتدى على

سره رفع دعوى يطلب فيها الكف عن التعدي على خصوصياته مع حقه في المطالبة بتعويض عن الضرر الذي لحق به.

هذا بشكل عام، أما اليوم ومع تزايد استخدام الحاسوب، وتوجه الدول نحو الحكومة الإلكترونية والتجارة الإلكترونية، واتساع انتشار الإنترنت والاعتماد عليه في المراسلات والاتصالات، وتفشي استخدام البريد الإلكتروني، فقد ظهر الحق في السرية الإلكترونية التي تحمي الملفات، والبطاقات، والبريد الإلكتروني، والاتصالات عبر الإنترنت، وهذا المبدأ يتعين احترامه من الحكومة والأفراد، إذ أقر أنه ليس للسلطات الحكومية مراقبة الاتصالات الإلكترونية إلا لضرورة تتعلق بالنظام، أو الأمن القومي، أو لحماية حريات وحقوق الغير، أو للوقاية من الجرائم، حيث لا يتم الكشف على الرسالة والمعلومة أو الاتصال إلا عن طريق السلطة القضائية أو السلطة الإدارية للأسباب المشروعة في الاطلاع، وتعتبر عملية مراقبة الاتصالات على الإنترنت أو محتوى البريد الإلكتروني أو الملف جريمة يتم المعاقبة عليها جنائياً بالحبس مدة سنة، كما تصادر الأدوات المستخدمة لاستراق أو تسجيل أو نقل المعلومات، ويحكم بمحو التسجيلات المتحصلة عنها.

2-تهديد الخصوصية

تعتبر الخصوصية(**Privacy**)من بين أكثر الموضوعات إثارة للجدل والاهتمام في عدد من الدول، فهي تمثل موضوعاً لآلاف الكتب والمقالات والبحوث، ولعل التطورات الأخيرة في الاهتمام بالخصوصية ناتجة عن الانتشار السريع لتكنولوجيا المعلومات في كل منحى من مناحي الحياة، فالزيادة في قوة الحاسبات الآلية والانخفاضات المثيرة في حجمها المادي وسعرها، خلقت دورة متسارعة يستخدم فيها كل من الفرد والمنظمات الحاسبات بصورة متزايدة، والنتيجة المترتبة على ذلك أن البيانات أصبحت متاحة أكثر من أي وقت مضى في شكل رقمي، فالمعلومات الرقمية أكثر سهولة وأقل تكلفة من المعلومات غير الرقمية للتداول والمعالجة والتخزين.وعلى الطرف الآخر لهذه التطورات والمزايا التي زينت عصر المعلوماتية كان هنالك تزايد في القلق على هذه المعلومات وعلى الخصوصية.(كيت ،1999، (13 – 15)).

وتعد فكرة الخصوصية وارتباطها بتقنية المعلومات هي الأولى من بين مسائل قانون الحاسوب، وهي الأولى في مناطق التساؤل عن أثر التقنية على النظام القانوني. وارتبطت ولادة فكرة الخصوصية بالخوف من المخاطر التقنية التي تهدد حياة الأفراد الخاصة، فتمس بشكل مباشر أسرارهم وخصوصياتهم.(عرب ،2002 ، (60 –61)).

والخصوصية هي حق من حقوق الأفراد، وأكثر ما يعطي هذا الحق قوة ودعماً هو أنه حق منحه الله عز وجل إلى عباده . وتتمثل الخصوصية "بحماية المعلومات الشخصية من التعرض للكشف بحيث يكون الدخول إلى هذه المعلومات أو الولوج إليها مقتصراً على مجموعة من الأفراد دون غيرهم.(حجازي، 2002 ،282).

وتعد أمريكا من أكثر الدول اهتماماً بها وهذا يؤكد الكم الهائل من التشريعات التي أصدرتها منذ السبعينات من القرن الماضي لحماية الخصوصية إلى يومنا هذا. ومن أهم هذه التشريعات (تشريع الخصوصية لعام(1974)و تشريع حماية الخصوصية لعام(1980) وتشريع خصوصية الاتصالات الإلكترونية عام (1986) وتشريع حماية الكمبيوتر لعام(1987) وتشريع تطابق خصوصية الكمبيوتر(1988) وتشريع حماية شبكات الإنترنت التي يستخدمها المستهلكون لعام(1997). (Turban & Others , 2000 , 345).

ويصاحب عملية انتهاك خصوصية المعلومات عدد من المشكلات تندرج تحت خمسة من المجالات:-

1-"التنصت : وهو التعرض للمعلومات وسرقة حسابات بطاقات الائتمان والمعلومات الخاصة بالحسابات".

2- " سرقة الأرقام السرية: وذلك للتمكن من السيطرة على الأجهزة والبرامج المختلفة".

3- "تعديل البيانات: وفيه تتعرض البيانات للهجوم من قبل المتطفلين حيث يقوم المتطفل بتعديل البيانات المخزنة أما من خلال التعامل المباشر أو من خلال برامج متخصصة للقيام بهذا العمل"

4-"الخداع: في هذه الحالة يقوم المتطفل بتقمص شخصية شخص آخر والتعامل على الشبكة بهذه الشخصية الجديدة ".

5-رفض الاعتراف عند القيام بالمعاملة التجارية الإلكترونية قد يرفض أحد الأطراف الاعتراف بالعملية بعد ان تتم واستفاد منها أحد الأطراف".

هذه هي مجالات المشكلات التي تصاحب انتهاك خصوصية المعلومات (عباس والفضلي ، 2001، 348) .

ومن معترضات الخصوصية أحد برامج الحاسوب هو برنامج (Cookies) كوكيز، وهو برنامج في أجهزة الحاسوب يتيح للشركات التي تمتلك المواقع على الإنترنت بأن تخزن وتطلع على كل ما تقوم به عندما تفتح جهاز الحاسوب الخاص بك. وعليه يتاح لهم الاطلاع على المعلومات الشخصية الخاصة بالأفراد، وعاداتهم وسلوكهم، وهواياتهم، وخططهم، ونمطهم الاستهلاكي. وقد يقدموا على بيع هذه المعلومات لشركات التسويق. وهنالك طريقتان للتخلص من كوكيز:

1-يستطيع مستعمل جهاز الحاسوب حذف كوكيز نهائياً، لكن هذا الحل مكلف جداً لمستعمل الجهاز، إذ يترتب عليه إعادة برمجة المواقع المراد زيارتها من جديد في كل مرة يود زيارتها، وهذا مكلف ويتطلب جهداً ووقتاً كبيرين، كما أنه حل غير عملي.

2- الحل الثاني، ويعد الأكثر عملياً، ويتمثل باستعمال برنامج مضاد "للكوكيز"وهذا البرنامج مجاني يتم الحصول عليه من خلال الشركات الكبرى مثل (مايكروسوفت، وماكينتوش) حيث يبطل هذا البرنامج مفعول الكوكيز، ويستطيع مستعمل الموقع أن ينتقل بين أجزائه دون أن تسجل تحركاته أو أخذ معلومات شخصية عن هذا المستعمل. (346 -347), (Turban & Others , 2000)) .

مبادئ حماية الخصوصية الفردية

هناك خمسة مبادئ للتعامل مع المعلومات الشخصية عند جمعها ونشرها :_

1-إشعار الفرد بأنه يتم جمع معلومات عنه.

2-أن يكون صاحب المعلومات هو صاحب القرار في كيفية استعمال المعلومات التي تم جمعها عنه.

3-أن يكون صاحب المعلومات قادراً على الاطلاع والوصول إلى المعلومات الخاصة به والمجموعة عنه بسهوله.

4-أن يحصل صاحب المعلومات على ضمانات لحماية المعلومات المجموعة عنه وعدم الاطلاع عليها من قبل أشخاص غير مخولين.

5-التأكد من وجود طريقه لتنفيذ هذه المبادئ ووجود سلطة يتم الرجوع إليها في حالة حدوث خلاف . (Turban & Others,2000,(347-348))

إرشادات مقترحة لحماية الخصوصية الفردية

هنالك تسعة اقتراحات ترشد لحماية الخصوصية الفردية:-

1-التفكير ملياً قبل إعطاء أية معلومات شخصية لأي موقع على الحاسوب.

2-تتبع كيفية استخدامهم لإسمك.

3-احفظ المعلومات الخاصة بك خارج الأرشيف .

4-ادخل بإسم مستعار أو بدون التصريح عن شخصيتك عند زيارة الموقع.

5-استعمل الحاسوب بدون كوكيز .

6-استعمل اسم مستعار في البريد الإلكتروني .

7-استعمل الرموز .

8-ابتعد في بريدك الإلكتروني عن عنوان عملك.

9-استفسر من مسؤولك أو مسؤول الحاسوب في عملك عن سياسة المنظمة المتعلقة بالخصوصية (Turban & Others, 2000 , 348)

القانون وحق الخصوصية

يعد احترام الحياة الخاصة من المبادئ الدستورية الثابتة حيث يقر الدستور بأن لحياة المواطنين الخاصة حرمة يحميها القانون فلكل شخص الحق في ان تظل أسرار حياته الخاصة محجوبة عن العلنية ومحمية من تدخل الغير واستطلاعهم. ويخرج عن نطاق الحياة الخاصة جوانب الحياة العلنية التي تتم بحضور الناس أو

مشاركتهم في الحياة العامة للجماعة التي يمكن ان تكون محلاً للنشر والتحقيقات الصحفية ولاشك في ان نطاق الخصوصية يختلف من الفرد العادي إلى الشخصيات العامة السياسية والفنية والأدبية حيث يزداد نطاق الخصوصية لشخصيات بسبب الشهرة.

وبقي الحق في الخصوصية حق معترف فيه في زمن المعلوماتية والحاسوب والشبكات وما صاحبه من تزايد صور الانتهاك والحق في الخصوصية في مجال المعلومات يعني حق الفرد في أن يقرر بنفسه متى وكيف والى أي مدى يمكن ان تصل المعلومات الخاصة به إلى الآخرين حيث يحمي القانون الحق في الحياة الخاصة وما يتعلق بها من معلومات مثل الصداقات والحالة الصحية والعاطفية والأسرية ويخرج عن ذلك المعلومات المتعلقة بالحياة العامة للشخص رغم صعوبة تحقيق خصوصية مطلقه للشبكات أو حماية كاملة لسرية البيانات على الشبكات بسبب تزايد مخاطر الانتهاك وتوسعه . (منصور ، 2002 ،(362 – 365))

3-تهديد التكاملية

لقد اختلفت طريقة طرح مصطلح التكاملية(**Integrity**) من عالم إلى آخر، فالبعض جعلها ملازمة لسلامة المحتوى، في حين اعتبرها البعض الآخر متلازمة مع الموجوديه. لهذا كان تفسير مصطلح التكاملية متنوع الزوايا، فقد فسرت على أنها(جودة المصدر أو درجة دقتها وكمالها وأصالتها ومصداقيتها فهي تدل على الحالة التي تؤكد أنها معلومات موثوقية أو اصليه ولا يمكن إنكارها من قبل الشخص الذي أرسلها أو عالجها).(البدا ينه ، 2002 ، 169) .

ومنهم من عبر عنها على أساس أنها سلامة المعلومات وتكاملها، ففسرها على (أنها التأكد من ان جميع البرامج التي يستخدمها النظام تقوم بعملها بشكل جيد ومترابطة فيما بينها وخالية من أية أخطاء ويتم الحصول على النتائج المطلوبة بشكل دقيق في الوقت الذي نكون بحاجة لها).(داود والمشهداني ،2001 ، 20) .

والبعض عبر عن التكاملية وسلامة المحتوى على أنها "التأكد من أن محتوى المعلومات صحيح لم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغييره عن طريق تدخل غير مشروع (عرب،2002،180) .

وحتى تحقق الأعمال الإلكترونية نجاحاً لا بد لها من تحقيق التكامل في عملها من خلال التنسيق المستمر بين الشبكات الداخلية والخارجية وكذلك من خلال تناسق الإجراءات، والممارسات، والاحترازات الخاصة بنظم المعلومات لكي تساهم في تحقيق حماية وأمنيه لأنظمة المعلومات. (البداينه ،2002،336).

فتعرض نظام المعلومات إلى أي تهديد لا بد ضمنياً من أن يفقده تكامليته، فينخفض تكامل النظام؛ وكذلك من شأن إجراء أي نوع من أنواع الحماية واستخدام أي سياسة أمنية من المساهمة في تحقيق التكاملية للنظام، وتدعيمها، والعمل على زيادتها.

أهم عناصر تكاملية حماية البيانات الشخصية

1-"البعد التقني للحماية :توفير أدوات حماية تقنية تضطلع بتقليص عمليات جمع البيانات الشخصية التي تتم دون علم المستخدم أو تمنعها وكذلك تقنيات تتيح للمستخدم التعامل مع البيئة الرقمية بقدر من التخفي ملائم لأغراض الاستخدام "

2-"البعد القانوني للحماية :توفير البناء القانوني الملائم لتنظيم مسائل الحماية ويشتمل ذلك تشريعات حماية البيانات الشمولية والقطاعيه ومدونات السلوك والتنظيم الذاتي لقطاعات الخدمة والإنتاج ووسائل الحماية التعاقدية كسياسات الخصوصية الملائمة التي تلزم بها جهات الخدمة التقنية نفسها أو عقود تبادل المعلومات المناسبة التي تبرم لتغطية نقل البيانات خارج الحدود للدول التي لا تتوفر فيها تشريعات الحماية الملائمة"

3-"البعد التوعوي للحماية:توفر وإشاعة استراتيجيات التعامل الإدارية والتنظيمية الملائمة من وعي المؤسسات والمستخدمين لتحقيق الحماية التعاملية المنطقية من وعي للمخاطر ووعي لوسائل تقليلها أو منع حصولها".(عرب،2002،112)

التشفير(Encryption)

يعتبر ضمان مستوى من (الموثوقية، والخصوصية، والتكاملية) ضد التهديدات هدفاً أساسياً لأنظمة الأمن والحماية؛ لأن في ذلك أمن لنظام بأكمله، ووسائل الحماية الفنية وغير الفنية لها دور كبير في توفير الحماية مع وجود تفاوت في أدوار هذه

الوسائل، ويعتبر التشفير الوسيلة الأكثر أهمية من وسائل الحماية، فهو من أكثر هذه الوسائل فعالية في توفير الأمن والحماية لأنظمة المعلومات.

وترجع أهمية دور "التشفير" في ميدان أمن المعلومات إلى أنه يمثل أكثر وسائل الحماية أهمية في تحقيق وظائف الأمن والسرية التكاملية وتوافر المعلومات في وقتها، فضمان السرية يعتمد على عدة وسائل أهمها التشفير لوسائل التثبت، وكلمات السر، وتشفير ترميز الملفات والمعطيات، وكذلك تعتمد حماية سلامة المحتوى على تشفير البيانات المتبادلة والتثبت لدى فك التشفير بأن الرسالة الإلكترونية لم تتعرض لأي نوع من التعديل والتغيير، وهو من أبرز وسائل عدم إنكار التصرفات عبر الشبكات .(عرب، 2002، 166)

إن معظم المعلومات العابرة عبر الإنترنت غير آمنة، فأي معلومة خصوصية يجب أن تكون مؤمنة عبر الإنترنت، ووسائل تأمين هذه المعلومات كثيرة، ولكن أكثرها فعالية "التشفير" إذ يتم تحويل النص إلى رموز لا يمكن فهمها أو قراءتها إلا من قبل المرسل والمستقبل، ويعتبر انتشار استخدام التشفير متزامناً مع ظهور الحاسوب، لكنه بصورته البدائية موجود منذ القدم، إذ استخدمه المصريون القدماء، وكتحديد دقيق للفترة الزمنية التي ظهر فيها التشفير لأول مرة، فقد كانت منذ أربعة آلاف سنة على الأقل حيث استخدمت منذ حوالي (900) قبل الميلاد في الرسومات المصرية التي كانت تستبدل الكتابة برموز من اللغة الهيروغليفية النظامية بشكل نقوش، وبعد أقل من (500) سنه انتشر التشفير في الصيغ والمستندات الدينية إضافة إلى الاتصالات الحكومية أما في الشفرات الحديثة، فإنهم يستخدمون النقاط والثقوب . (Deitel & Others ,2001 ,199) و(بانكس ، 2001 ، 116)

(التشفير) لفظاً هو الحديث حيث كان في السابق يستخدم اللفظ العربي الذي يصف عملية التشفير (بالتعميمة) فهو يشير إلى الرسائل المشفرة، ويعد التشفير من أهم وسائل الحفاظ على أمن المعلومات في بيئة غير آمنة، فيتم عن طريقه تحوير صورة البيانات إلى صورة غير مفهومه لمن يحاول السرقة أو التنصت، أو التلصص عليها، ومن ثم فهو يحقق سرية البيانات وخصوصيتها، مما يساهم في

تحقيق سلامة هذه البيانات، لأن البيانات التي لا يمكن قراءتها وفهمها لا يمكن تعديلها أو تزييفها أو نشرها. (داود ، 2000 ، 176)

أما فك التشفير، فهو العملية التي تتم خلالها إعادة الرسائل المشفرة إلى وضعها الأصلي السابق قبل التشفير.

ومن أبرز التهديدات التي يمكن التغلب عليها بوساطة التشفير مايلي:(داود ،2000، 178).

1-الإطلاع على المعلومات السرية المحظورة .

2-محاولات الاعتداء على البيانات المتداولة عبر الشبكات وتعديلها.

3-تغيير مسار البيانات وتوجيهها إلى وجهه أخرى.

4-إعاقة وصول بعض الرسائل في وقتها وتأخيرها .

5-العبث بمحتويات الرسائل المتبادلة وتغيير مضمونها .

6-تحميل الرسائل المنقولة عبر الخط رسائل زائفة .

7-تغيير كلمات السر التي يستخدمها المستفيدون .

8-انتحال شخصية المستخدم الحقيقي .

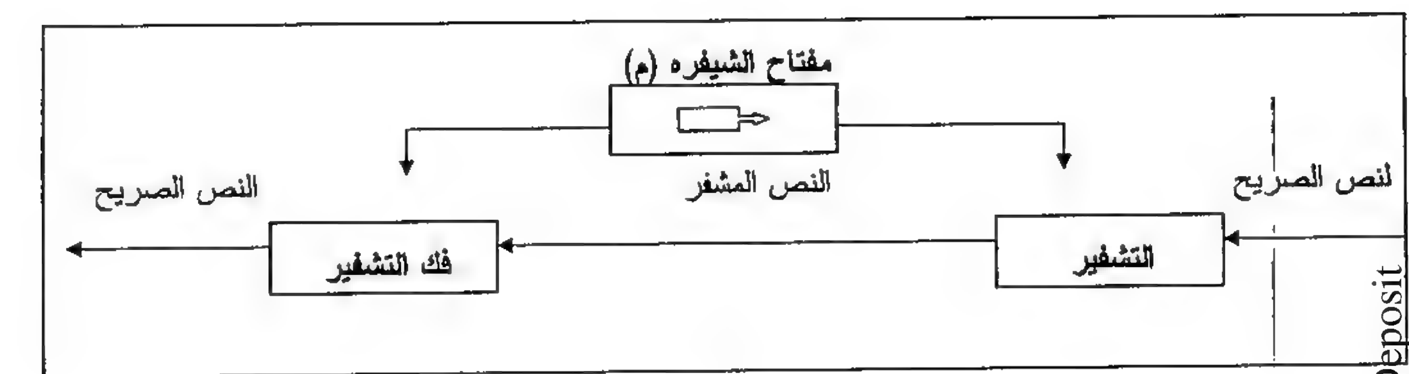
9-العبث بالبيانات المخزنة على الحاسبات نفسها والقيام بتعديلها.(البداينة، 2002 ، 355)

أنواع التشفير

يتم التشفير بشكل عام من خلال نوعين رئيسيين هما:

أ-المفتاح السري للتشفير "التشفير المتماثل" ويستعمل بين المنظمات مع بعضها البعض، وذلك باستخدام شيفرة بين أطراف التشفير (المستقبل والمرسل) حيث يكون المستقبل والمرسل هما فقط من يعرف فك الشيفرة، وهذا النوع يستخدم فقط بين طرفين أو شخصين في المنظمة نفسها، لكن مشكلته تتمثل في اضطرار أحد أطراف التشفير إلى إرسال الشيفرة عن طريق مراسل إلى الطرف الآخر مما يؤدي إلى عدم ضمان الأمان الكامل في الإتصال خصوصاً إذا وقعت الرسالة خطأً في يد المستقبل. (Deitel & Others ,2001,200)

وسمي هذا النوع التشفير المتماثل، لأنه يستخدم مفتاح شيفرة واحد لكل من عملتي التشفير وفك التشفير، والشكل التالي يوضح ذلك.



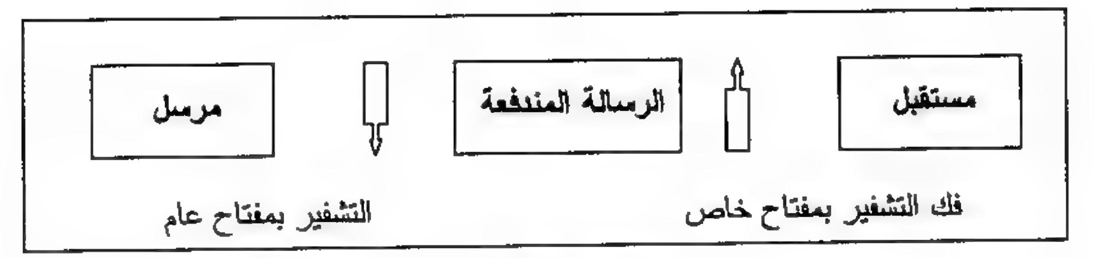
الشكل رقم (4)

التشفير المتماثل

المصدر :(داود ، حسن طاهر ، (2000)، الحاسب وأمن المعلومات، ط1، معهد الإدارة العامة، الرياض ، ص 177)

ب-المفتاح العمومي للتشفير" التشفير غير المتماثل "إذ تم عام(1976) تطوير المفتاح العمومي لكتابة الشيفرة عن طريق الباحثين (وايت فيلب ومارتن هيلمن) من جامعة ستانفورد، وذلك لحل مشاكل الأمان في عمليات التبادل التجاري، وتتسم عملية التشفير باستخدام مفتاح التشفير العمومي ومفتاح الشيفرة الخصوصي، حيث يبقى المفتاح الخصوصي فقط بحوزة المالك الشخصي، في حين يمكن ان يكون المفتاح العمومي متوافراً لدى جميع الموظفين، وبذلك تكون قراءة الرسالة ممكنة فقط من قبل المستقبل. وعليه، فإن الشيفرة التي تكون بحوزة المالك الشخصي هي ذات الأهميـــة الكبرى. ويتيح استخدام هذه الطريقة في التشفير للمستقبل التحقق من شخصية المرسل باستخدام الشيفرة الخصوصية للمرسل عبر قراءة الشيفره عن طريق تحليل الشيفرة العمومية للمنظمة، ومن ثم يصبح من الممكن التحقق من المرسل والمستقبل عند استخدم الشيفرة العمومية والخصوصية .(Deitel & Others,2001 ,202)

وأطلق على هذا النوع تسمية التشفير غير المتماثل، لأنه يستخدم مفتاحين أحدهما للشيفرة، والآخر لفكها، كما يوضح الشكل التالي:



الشكل رقم (5)

التشفير غير المتماثل

المصدر: (LAUDON, KENNETH C &. LAUDON, JANE P), (2000), MANAGEMENT INFORMATION SYSTEMS, Prentice-Hall, Inc ,P.512)

من أكثر ما يميز هذه السياسة الأمنية أنها متطورة بشكل مستمر فهي تواكب التطورات الحاصلة في تقنية المعلومات وتعد الشيفرة اكثر أماناً كلما كانت طويلة ومعقدة حيث يصعب فكها من قبل المعتدين .

وبعد هذا العرض لمصادر التهديد ونتائجه وبعض وسائل الحماية لأمن المعلومات، فإن الوسائل الفنية وغير الفنية وحدها لا تكفي لتحقيق حماية لأنظمة المعلومات، إذ لا بد من تكامل جهود كل من الإدارة، والقانون، والموظف، والمواطن بحيث تعمل الإدارة على التخطيط، والتنظيم، واتخاذ القرارات، وتراقب، وتضبط، وتصدر الإجراءات والوسائل، وتعمل على مراقبة الالتزام بها، وبتطبيقها، في حين يتولى القانون إصدار التشريعات، وتحديد الجزاء المترتب على ارتكاب اختراقات أو سرقات أو إفشاء أسرار أو ارتكاب جرائم معلوماتية، كما يحقق في حالة حدوث جريمة، ويساهم في كشف الفاعل والمسبب الحقيقي .

أما الموظف؛ فإن تمتعه بأخلاقيات وظيفية واجتماعية عريقة، يردعه عن ارتكاب عمل غير مشروع وغير أخلاقي، كما يساهم تدريبه وتوعيته في زيادة فهمه لعمله والى خطورة إقباله على عمل غير مشروع يلحق ضرراً بالمنظمة، وبنفسه وبالمجتمع كله، مما يحول دون ارتكابه لأخطاء مقصودة أو التلاعب والتحرش بأنظمة المعلومات واختراقها، ويعزز من تقيده واحترامه للقوانين والتشريعات والأنظمة الصادرة عن الجهات المسؤولة .

أما المواطن؛ فله دور كبير من خلال احترامه لحريات الآخرين، وعدم العبث بها أو الاعتداء عليها، وكذلك من خلال احترامه لأنظمة المنظمات التي يتعامل معها والأنظمة الخاصة بالدولة بشكل عام. ويؤكد ذلك أن عملية الحماية عملية متكاملة تحتاج إلى تعاون من جميع الأطراف، وهذا التعاون يتحقق من خلال بناء جسور متينة من الاتصالات المبنية على الشفافية والثقة بين المواطن والحكومة من جهة وبين الرئيس والمرؤوس من جهة أخرى، وذلك من خلال الاتصال متعدد الاتجاهات الذي يعتمد على المصداقية والشفافية وفي النهاية يقود هذا إلى بناء الثقة والتعاون والتماسك، وهذا ما يحتاج إليه كل كيان ومشروع، وبخاصة في مراحله الأولى مثل مشروع الحكومة الإلكترونية .

ثانياً: الدراسات السابقة

الدراسات العربية

دراسة قام بها (العوامله ، 2002) "الموسومة بالحكومة الإلكترونية ومستقبل الإدارة العامة : دراسة استطلاعية للقطاع العام في دولة قطر".

وهدفت هذه الدراسة إلى تحليل مفهوم الحكومة الإلكترونية، والتعرف على أهم معوقاتها، وأهم متطلبات تنفيذها، إذ اعتمدت هذه الدراسة على الأسلوب النظري والتطبيقي من خلال المسح المكتبي لأدبيات هذا الموضوع، والمسح الميداني لآراء عينة موظفي القطاع العام في دولة قطر، وشملت عينة الدراسة(500) موظف حكومي استجاب منهم (287) بشكل قابل لتحليل .

وتوصلت الدراسة إلى جمله من النتائج أهمها ندرة الأدبيات الخاصة بموضوع الحكومة الإلكترونية خصوصاً في الأدبيات العربية، وعدم وجود اتفاق على مفهوم الحكومة الإلكترونية، وكان هناك ما نسبته(78%) من المبحوثين على قناعة تامة بضرورة التحول نحو الحكومة الإلكترونية. كما توصلت الدراسة إلى وجود معوقات لتنفيذ الحكومة الإلكترونية أهمها بالترتيب: ضعف الوعي الاجتماعي؛ ونقص التمويل؛ ونقص العناصر البشرية؛ ونقص المعلومات، ونقص التكنولوجيا، وتخلف التشريعات. وقد حصل ضعف الوعي الاجتماعي على أعلى

نسبة (78%)، كما أكدوا على أهمية جمله من المتطلبات للتحول نحو الحكومة الإلكترونية مرتبة حسب أهميتها: التخطيط الاستراتيجي، وتعليم القوي البشرية وتدريبها؛ وإنشاء نظام وطني للمعلومات؛ وتطوير التشريعات وتحديثها؛ ووفرة التمويل؛ والتحول التدريجي، وقد حصل التخطيط الاستراتيجي على أعلى نسبة (88%).

وكانت أهم التوصيات أن مفهوم الحكومة الإلكترونية مفهوم متكامل، ويحتاج التحول نحوها إلى إحداث تغييرات جذرية هيكلية سلوكية تشريعية تنظيمية في المنظمات، ويجب الحرص على نشر توعية جماهيرية لمفهوم الحكومة الإلكترونية من خلال إجراء تعديلات على خطط وبرامج أنظمة الإعلام، والتربية والتعليم، والمعلومات، والاتصالات مع ضرورة الحرص على التحول التدريجي في مشروع الحكومة الإلكترونية .

دراسة (أبو موسى، 2002)الموسومة " جرائم الكمبيوتر : هل يمكنك حماية نظام المعلومات المحاسبية الخاص بك؟ "

وهدفت هذه الدراسة إلى التحقق من المخاطر الأمنية التي يجب أخذها بالاعتبار، وتتحدى أنظمة المعلومات المحاسبية(CAIS) في صناعة البنوك المصرية وأيضاً طرق التحكم المحتملة، المطبقة فعلاً لمنع الثغرات الأمنية وكشفها.

وقدم منظومة أسئلة منتقاة استخدمت لاستطلاع آراء رؤساء أقسام التدقيق (HOIAD) ورؤساء أقسام الكمبيوتر(HOCD) في صناعة البنوك المصرية بالنظر إلى قضايا أنظمة المعلومات المحاسبية في بنوكهم :

1- صبغة أو طابع أنظمة المعلومات المحاسبية(CAIS) في صناعة البنوك المصرية.
2- المخاطر الأمنية التي يجب أخذها بالاعتبار والمؤثرة في أنظمة المعلومات المحاسبية (CAIS) في صناعة البنوك المصرية .
3- طرق التحكم المحتملة المطبقة للقضاء على المخاطر الأمنية أو التقليل منها في صناعة البنوك المصرية .

وتم استطلاع آراء جميع قطاع البنوك(إدارة 66 بنكاً) في قطاع البنوك المصرية، واستعملت(79) سؤالاً في منظومة أسئلة جمعت من إدارة(46) بنكاً. إذ إن(46) أجاب عنها رؤساء أقسام الكمبيوتر، و(33) سؤلاً تمت إجابتها من قبل رؤساء أقسام التدقيق الداخلي، وكانت درجة الإجابة عند رؤساء أقسام الكمبيوتر بعد استبعاد البنوك المندمجة والمسيلة أو المصفاة، وغير المحوسبة(79.3%) بينما كانت الدرجة عند رؤساء أقسام التدقيق الداخلي(56.9%) .

وناقش الباحث المخاطر الرئيسة التي تهدد أنظمة المعلومات المحاسبية(CAIS) وكفاية أنظمة الحماية المطبقة في البنوك المصرية .

وأدى الاختلاف بين المجموعتين المجيبتين للاستطلاع وأيضاً بين أنواع البنوك بالنظر إلى المخاطر الرئيسية وإجراءات الحماية المضادة المطبقة إلى الكشف عن أنظمة الحماية غير الملائمة وغير الكاملة، وتم تقديم بعض الاقتراحات لتقوية نقاط ضعف أنظمة الحماية في قطاع البنوك المصرية .

وفي دراسة (الشواف والزلزلة ، 1999) الموسومة " قياس تكامل المعلومات : في دراسة استكشافية مطبقة على المنظمة الكويتية"،شمل مجتمع الدراسة المنظمات الكويتية الحكومية والخاصة جميعها التي يوجد لديها إدارات لنظم المعلومات تحت أي مسمى، إذ استهدفت هذه الدراسة إجراء مسح للمستويات الحالية لتكامل المعلومات لنظم المعلومات القائمة في المنظمة الكويتية من وجهات نظر متعددة ، مع التركيز على تحديد نقاط الضعف التي تهدد التكامل الكلي للمعلومات حتى يمكن تلافيها أو تقليلها .

وتوصلت الدراسة إلى نتائج تشير إلى وجود مشاكل تتعلق بتكامل المعلومات في بيئة إدارة المعلومات المؤتمتة في المنظمات الكويتية بشقيها الحكومي والخاص، كما أكدت على دور إدارة الكوارث في زيادة تكامل المعلومات ، ولكن النتائج، وبناء على وجهة نظر الإدارات المستفيدة، أظهرت أن مستويات ضعف تكامل المعلومات في القطاع الحكومي أعلى بصورة ملحوظة منها في قطاع الشركات الخاصة ، وذلك لأن قطاع الشركات يحرص على تقديم أفضل مستوى من الخدمات للعملاء لذلك يجب ان يكون تكامل المعلومات مرتفعاً، وكان من أبرز أسباب

التهديدات لتكامل المعلومات أسباب تنظيمية تحول دون سرعة الاستجابة لطلبات المستخدمين، وعدم تحديد الجهات المسؤولة عن توفير المدخلات، وعدم وجود نظم ضبط ورقابة فاعلة أو ضعفها إن وجدت، وعدم كفاءة العاملين في قسم نظم المعلومات. وتبين الدراسة مجموعة من التوصيات المحددة لتمكين المديرين والممارسين من صياغة إطار علمي لرفع مستوى تكامل المعلومات في المنظمة الكويتية .

وهناك دراسة (البياتي ، 1996) الموسومة "الوسائل الفنية لحماية البرامج ودور التشريع في حماية المعلومات".

وهدفت هذه الدراسة إلى تحديد عناصر أمن الحواسيب وأسس التصنيف لتحديد مستوى الأمنية، كما تناولت الوسائل الفنية وغير الفنية لحماية الحواسيب، وأبرزت دور التشريع القانوني في حماية المعلومات.

وتم فيها إجراء مسح على عدد من الدوائر الحكومية والمؤسسات والشركات في العراق، بهدف التعرف إلى نسبة المؤسسات والشركات التي تعتمد أنظمة أمنية وخطط وسياسات أمن وحماية، وإلى معرفة أكثر التهديدات أهمية وإثارة لاهتمام المستخدمين، وهي الإجراءات الأمنية التي تم التركيز عليها لمواجهة التهديدات الأمنية للمؤسسات والشركات.

وكان من أبرز نتائج المسح ما يلي:-

أن الحاجة إلى الأمنية معترف بها رسمياً في معظم المؤسسات والشركات المشمولة بالمسح، إذ ظهر أن أكثر من ثلثي المشمولين لديهم سياسات وخطط أمنية، وأكثر من(75%) لديهم أشخاص أو دوائر مسؤولة عن وظيفة الأمن، وأن(75%) من المشمولين كانت لديهم خطط لاسترجاع المعلومات والبرمجيات في حالات الأحداث الطارئة، وأن الأكثرية أوضحت أن ما يشغلهم، بالدرجة الأولى، هو منع الوصول إلى الأنظمة من قبل غير المخولين، وكذلك منع استخدام غير المخولين لمخازن الأنظمة والملفات المخزونة خارج الموقع، ومنع الوصول إلى برمجيات السيطرة كإجراءات أمنية في الوقت الذي لم تأت مخاطر الفيروسات بالمرتبة الأولى للمشاكل والتهديدات مع أن حوالي(20%) من المشمولين أظهروا اهتمامهم

بالفيروسات، ولكن(50%) من المواقع المشمولة لديها معدات مضادة منصوبة على الحواسيب المستعملة. أما بالنسبة للإجراءات الأمنية التي أعطيت أهمية قصوى من قبل الإجابات ، فكان(53%) من الاستجابات لخزن نسخ إضافية للمعلومات والبرمجيات خارج الموقع في المرتبة الأولى من ناحية الأهمية ، كما تبين أن مصدر الاعتداء والتهديد في أغلب الأحيان يأتي من داخل المنظمة وليس من خارجها حيث توصل من خلال المسح ان بين(70 – 80%) من الاعتداءات هي داخلية.

وأهم التوصيات أنه لابد لأي بلد من وضع أسس ومعايير لتحديد المستوى الأمني لمنظومات الحواسيب ، وإعطاء أهمية كبيره للوسائل غير الفنية في حماية المعلومات التي لا تقل أهمية عن الوسائل الفنية للحماية ، وعلى كل دولة إصدار تشريع دقيق وواضح لمعالجة الاعتداء على المال المعلوماتي .

الدراسات الأجنبية

دراسة (Kankan Halli & Others, 2003) بعنوان " الدراسة المتكاملة للفاعلية الأمنية لأنظمة المعلومات " .

وهدفت هذه الدراسة إلى تطوير نموذج متكامل للفاعلية الأمنية لنظام المعلومات، وفحص هذا النموذج بشكل عملي. وذلك بعمل استبانة وزعت على مديري أنظمة المعلومات في قاعات اقتصادية مختلفة، وقد تم استخدام النسب والمتوسطات وقيم ألفا في عملية تحليل البيانات، وتوصلت الدراسة إلى أن المشروعات الصغيرة والمتوسطة الحجم تمارس نشاطات رادعة أقل من المنظمات الكبيرة في سبيل ضمان الأمن لنظام المعلومات، وأن المنظمات التي تدعم إدارتها العليا نظام المعلومات تمارس إجراءات (نشاطات) وقائية اكثر من المنظمات التي لا تدعم إدارتها العليا نظام المعلومات. وتوصلت الدراسة أن المنظمات المالية تقوم بجهود رادعة ومتشددة على أمن المعلومات أكثر من المنظمات الأخرى، وان الجهود الرادعة والوقائية لحماية المعلومات تعمل على تعزيز الفاعلية الأمنية لنظام المعلومات.

دراسة أخرى قام بها (Salem, 2003) بعنوان " فوائد القطاع العام والخاص من الحكومة الإلكترونية":

وهدفت هذه الدراسة إلى التعرف على الخلاف الذي يدور حول الموقع الإلكتروني الحكومي المرتبط بوزارة الطاقة، وكذلك التعرف إلى حدود كل من الحكومة الإلكترونية والتجارة الإلكترونية ، إذ ترتبط الحكومة الإلكترونية بنشاطات القطاع العام بينما ترتبط التجارة الإلكترونية بالقطاع الخاص ، فقد ظهر القلق لدى مندوبي الحاسوب والبرمجيات وشركات الاتصال من وجود الحكومة الفدرالية في الأسواق الإلكترونية المنشأة وفي سوق تزوير المعلومات بالرغم من الاتجاه نحو خصخصة النشاطات الحكومية في إدارة كلينتون التي عملت على إعادة اكتشاف الحكومة .

وقد توصلت الدراسة إلى أنه في الوقت الذي تتطور فيه الحكومة الإلكترونية باتجاه أداء (القيام) بالعمل الحكومي ، وأن الدعم الذي تقدمه الحكومة الإلكترونية يعطي القطاع الخاص فرصاً أكثر لزيادة إنتاجه اعتماداً على المعلومات والخدمات التي تقدمها الحكومة ، وهذا يشجع على استخدام تكنولوجيا المعلومات واستغلال الفرص التي تعود على عملهم، وأن تجديد التوجيهات السياسية والتشريعية مع وضع قيادة محددة للحكومة الإلكترونية ربما يحدد ذلك دور الحكومة في زيادة التواصل الأمريكي.

وفي دراسة (chen & Gant, 2001) بعنوان " التحول المحلي لخدمات الحكومة الإلكترونية: استخدام تطبيقات(برمجيات) تزويد الخدمة " .

(خدمات الحكومة الإلكترونية المتحولة محلياً) (برمجيات الخدمات المزورة) هدفت هذه الدراسة إلى التعرف على قدرة برمجيات الخدمات المزودة على تحويل خدمات الحكومة الإلكترونية للمستوى المحلي، وذلك باستخدام نموذج يمكن الحكومات المحلية من التغلب على مصاعبها التي قد تتمثل بنقص المهارات ومحدودية المصادر المالية اللازمة لتطبيق البرمجيات المزودة للخدمة. وضمن النموذج الذي اعتمدت الدراسة، فإن هناك خمسة شروط تدعم القرار المتعلق باستخدام البرمجيات المزودة للخدمة، وهذه الشروط :

1-قوة دعم الإدارة العليا لهذه البرمجيات .

2-التنبوء بتحقيق عوائد بكفاءة عالية.

3- توافر تكنولوجيا معلومات للقسم الحكومي المسؤول عن ذلك

4-التقليل من قيود (ثقل) القانون والإجراءات .

5-اختيار برمجيات مزودة للخدمة تكون ذات نوعية جيدة .

وتوصلت الدراسة إلى أنه لضمان نجاح مشروع برمجيات الخدمات المزودة على الصعيد المحلي، يجب بناء تكنولوجيا معلومات مناسبة، وتقييم البرمجيات وفق ذلك ، وأن الإدارة يجب أن تركز على خدمة المواطنين وقطاع الأعمال، وذلك بالحوار مع المواطنين ورجال الأعمال للتعرف إلى احتياجاتهم وإدارة الصفقات المتعلقة بشراء برمجيات الخدمات، وكذلك توفير دعم الإدارة العليا للبرمجيات التي تقدم الخدمات، وذلك لاحتواء المعارضة التي قد تكون في بداية تكوينها لضمان التعاون والاتصال بين الدوائر المختلفة .

وهناك دراسة (Layne & Lee, 2001) بعنوان "التطوير العملي للحكومة الإلكترونية (نموذج الأربع مراحل) " .

وتهدف هذه الدراسة إلى وصف المراحل المختلفة لتطور الحكومة، الإلكترونية واقتراح نموذج حكومة من أربع مراحل لتطورها. وقد تم عمل هذا النموذج بالرجوع لمواقع حكومية مختلفة، فكانت المراحل التي شملها النموذج خلاصة التغير في وجهات نظر متعددة حول الهياكل الحكومية ووظائف الحكومة، التي أدت إلى حدوث تغير في الحكومة الإلكترونية وفي كل مرحلة من مراحل تطورها .

وتطرقت الدراسة إلى التحديات التكنولوجية والتنظيمية التي ترافق كل مرحلة من مراحل تطور الحكومة الإلكترونية، وقد وضعت الدراسة الكيفية التي تصبح بها الحكومة الإلكترونية منسجمة مع هيكل الإدارة العامة التقليدي . وخلصت الدراسة إلى التأكيد على أهمية المواطن ، باعتباره مستخدماً ومستفيداً من خدمات الحكومة الإلكترونية، والحث على ضرورة الوصول المحدد للخدمة، والتركيز على قضايا

السرية والخصوصية بما يوازي التركيز على المواطن مع الأخذ بالاعتبار مدى تطور الحكومة الإلكترونية.

ودراسة (Beheruz & CynthiaC , 1999)الموسومة (الاتصالات الإلكترونية في الجامعات والكليات : هل تتميز بالخصوبة) .

وجرت هذه الدراسة على الكليات والجامعات التابعة ل(AACSB) وتم استرجاع استبيانات من (134) جامعة وكلية قابلة للتحليل وهدفت هذه الدراسة إلى التعرف على مدى وجود سياسة خاصة بالاتصالات الإلكترونية في المناخات الأكاديمية للمديرين في عمليات دخولهم إلى الاتصالات والرسائل الإلكترونية الخاصة بالهيئة التدريسية، والإدارية، والكادر الوظيفي، والطلبة، كما تم حصر أبرز الأسباب وأهمها التي يعتقد المجيبون عن الاستبيان أنها أسباب مقنعة تقف وراء دخول الإداريين إلى الاتصالات الإلكترونية الخاصة بالهيئة الإدارية والتدريسية والطلبة وهل يحق لموظفي الجامعة على الصعيدين الأخلاقي والقانوني مراقبة ورصد البريد الخاص للهيئة التدريسية، والإدارية، والكادر الوظيفي والطلبة، كما تم الاستطلاع حول ما إذا كان هناك فرق بين خطورة الاطلاع على بريد الطلبة وبريد الإدارة .

وبعد التحليل تم التوصل إلى النتائج التالية أن هنالك (58.2%) من الجامعات والكليات التي شملها الاستطلاع توجد لديها سياسة خاصة بالاتصالات الإلكترونية، وأن (46%) من المستجيبين أقروا بأن هنالك حقاً للإداريين في الاطلاع على الاتصالات الخاصة بالموظفين والطلبة مع وجود تفاوت في أسباب الموافقة على إجازة الاطلاع على الاتصالات، فمنهم من وافق على السماح بالاطلاع كاستجابة لمتطلبات المحكمة والقضاء، أو في حالات إثبات أو الاستدلال على الأنشطة غير المشروعة، ومنهم من وافق في حالة وجود أي تهديد لحياة الأفراد أو في الوقت الذي يكون الهدف هو التحقق من شكوكات حول وجود شخص ما يتبادل المعلومات السرية مع أشخاص غير مصرحين ، هذا وأكد(87%) من المستجيبين عدم وجود فرق في خطورة الاطلاع على بريد الطلبة أو الإدارة، و(13%) منهم أكدوا على عدم الضرورة لوجود خصوصية لاتصالات الطلبة .

وأوصت الدراسة بضرورة توافر سياسة خاصة لكل منظمة تنظم الاتصالات الإلكترونية فيها مع ضرورة تحديد الحالات التي يسمح فيها بالاطلاع على الاتصالات الخاصة لكل من الإدارة والهيئة التدريسية والكادر الوظيفي والطلبة وضرورة التفريق بين حساسية وخطورة الاطلاع على بريد الإدارة والهيئة التدريسية والكادر الوظيفي والطلبة .

ودراسة مقارنة قدمها(Detmar W, 1996) الموسومة (بالتعامل مع المخاطر التي تواجه أنظمة المعلومات : نماذج التخطيط الأمني واتخاذ القرارات الإدارية) .

وأجرت هذه الدراسة مقارنة بين شركتين هما شركة(Customer Data , Inc) وشركة(Customer Processing Co) واستخدمت الدراسة لجمع المعلومات الاستبانة والمقابلات، وهدفت هذه الدراسة إلى التعرف على دور وعي المديرين، ومعرفتهم بآليات الرقابة في التعامل مع المخاطر التي تواجه أنظمة المعلومات، كما سعت إلى تحديد الأسلوب الذي يمكنه التعامل مع المشكلة بكفاءة .

وكانت نتائج الدراسة تؤكد أهمية استخدام نماذج تخطيط أمني تعتمد على تحليل الخطر أو التهديد، وضرورة التثقيف والتدريب حول موضوع الوعي الأمني مع الحرص على الاعتماد على مصفوفة إجراءات مضادة لتلك التهديدات، وهي أهم النماذج والنظريات التي يمكن استخدامها في التخطيط الأمني " نموذج اتخاذ القرارات الإدارية لسايمون" إذ يقوم هذا النموذج على عدة توجيهات فيما يخص المراحل العامة لمنهج التخطيط الفعال والذي يقوم على أساس خمس مراحل هي :-

1-التعرف إلى المشكلة الأمنية: إذ يتم تحديد المشكلة ووضع صياغة للتهديدات الخاصة باختراق أنظمة المعلومات .

2-تحليل التهديد والخطر: وهذه الخطوة إلزامية وضرورية بالنسبة لمجالات المشكلة التي تم تحديدها، إذ تساهم في تحديد الأخطار ووضع أولوية لها.

3-البدائل: يتم تحديد أولوية للمخاطر والتهديدات، وفي ضوئها يجري وضع حلول عدة لمواجهة احتياجات الشركة حسب ما ظهر عندما تم تحليل الخطر.

4-القرارات: وتتم المواءمة بين التهديدات والحلول المناسبة ، وانتقاء الخطط الأمنية ووضعها ضمن سلم الأولوية .

5-التطبيق: وتتم ترجمة الخطط ودمج الحلول المطروحة في الواقع الأمني الحالي الخاص بالشركة.

أما حول تطبيق مصفوفة الإجراءات المضادة على المشكلة ، فقد تم التوصل إلى أربعة إجراءات مضادة هي:-

1- الردع 2- الوقاية 3- الكشف 4- العلاج

ومن أهم التوصيات ضرورة تحرير موارد المنظمة لكي تستخدم في مراقبة الإجراءات التي لا يمكن وضع صياغة لها، كما أوصت بضرورة تبني خبراء الحماية والأمن آلية وسياسات تستند إلى نظريات في مجال التخطيط الأمني مع أهمية كسب دعم الإدارة العليا في مجال الأمن والحماية، والحرص الشديد على تقديم تدريب أمني للعاملين، وتثقيفهم حول المبادئ النظرية والعملية للأمنية والحماية .

دراسة قام بها(دونك ودويفينودين،1996) الموسومة بـ "الخصوصية كسياسة : من منظور تطبيق السياسات الخاصة لحماية البيانات على مستوى القاعدة في هولندا" ؛ وتطرقت الدراسة إلى حماية البيانات في هولندا، وقانون الخصوصية الهولندي الذي يطبق على سجلات البيانات الشخصية الآلية واليدوية ، إذ أجرى مسح شامل لـ(500) مراقب بيانات في القطاعات الثلاثة: (القطاع العام، وشبه العام، والقطاع الخاص) ، واقتصر المسح على عينة عشوائية. وأشارت النتائج إلى وجود مراقبي البيانات الأكثر التزاماً بالقوانين في القطاع العام، وأن مراقبي البيانات الذين يراقبون السجلات المتضمنة البيانات الحساسة يوجدون في مؤسسات القطاع شبه العام بنسبة(77%) من المؤسسات ، كما أن(66%) من المجيبين أكدوا أهمية مبادئ حماية البيانات في قانون الخصوصية الهولندي، ولم يظهر أي تأثير لمستوى التعليم، ولا الجنس، ولا العمر على درجة الدعم لمبادئ الحماية، وأوصى الباحث بضرورة تحقيق تكيف للقوانين مع الآليات المحددة بموجب البيئة ومراعاة الفروقات بين القطاعات المختلفة من ناحية بيئتها وإمكانياتها ، واقترح استخدام مراحل تطبيق مناسبة لتسهيل عملية السيطرة على التصرفات اللائقة مع المعلومات.

ثالثاً: أسئلـــة الدراســـة وفرضياتها

أسئلة الدراسة

تحاول هذه الدراسة الإجابة عن الأسئلة التالية:

1-ما هي تصورات المبحوثين لمصادر التهديدات الخارجية لأمن المعلومات فـــي العمل الحكومي ؟

2-ما هي تصورات المبحوثين لمصادر التهديدات الداخلية لأمن المعلومـــات فـــي العمل الحكومي ؟

3-ما هي تصورات المبحوثين للنتائج المباشرة لتهديدات أمن المعلومات؟

4-ما هي تصورات المبحوثين للنتائج غير المباشرة لتهديدات أمن المعلومات؟

5-ما هي طبيعة العلاقة بين متغيرات الدراسة المستقلة والتابعة؟

6- ما هي الأهمية النسبية للبنية التحتية(تنظيمية، تقنية، قانونية) لأمنية المعلومات الإلكترونية.

فرضيات الدراسة

1-لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الداخلية لأمن المعلومات ببعديها (التهديدات التقنية والتهديدات البشرية) على النتائج المباشرة للتهديدات.

أ-لا يوجد أثر ذو دلالة إحصائية للتهديدات التقنية على النتائج المباشرة للتهديدات .

ب-لا يوجد أثر ذو دلالة إحصائية للتهديـــدات البشـــرية علـــى النتـــائج المباشـــرة للتهديدات.

2-لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الداخلية لأمن المعلومات ببعديها (التهديدات التقنية والتهديدات البشرية)على النتائج غير المباشرة للتهديدات .

أ-لا يوجد أثر ذو دلالة إحصائية للتهديدات التقنية علـــى النتـــائج غيـــر المباشـــرة للتهديدات .

ب-لا يوجد أثر ذو دلالة إحصائية للتهديدات البشرية على النتائج غيـــر المباشـــرة للتهديدات.

3-لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الخارجية لأمن المعلومات بأبعادها

(الكوارث الطبيعية ، المحترفين والقراصنة ، البرمجيات الخبيثـــة) علـــى النتـــائج المباشرة للتهديدات.

أ- لا يوجد أثر ذو دلالة إحصائية للتهديدات (الكـــوارث الطبيعيـــة) علـــى النتـــائج المباشرة للتهديدات.

ب- لا يوجد أثر ذو دلالة إحصائية للتهديدات (المحترفين والقراصنة) على النتـــائج المباشرة للتهديدات.

ج- لا يوجد أثر ذو دلالة إحصائية للتهديدات (البرمجيات الخبيثـــة) علـــى النتـــائج المباشرة للتهديدات.

4-لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الخارجية لأمن المعلومات بأبعادها (الكوارث الطبيعية ، والمحترفين والقراصنة ،و البرمجيات الخبيثة) على النتائج غير المباشرة للتهديدات.

أ- لا يوجد أثر ذو دلالة إحصائية للتهديدات (الكوارث الطبيعية) على النتائج غيـــر المباشرة للتهديدات.

ب- لا يوجد أثر ذو دلالة إحصائية للتهديدات (المحترفين والقراصنة) على النتـــائج غير المباشرة للتهديدات.

ج- لا يوجد أثر ذو دلالة إحصائية للتهديدات (البرمجيات الخبيثة) على النتائج غير المباشرة للتهديدات.

5-لا تختلف تصورات المبحوثين لنتائج التهديدات الأمنية باختلاف المتغيرات الديموغرافية هي: "الجنس، والعمر، والمؤهل العلمي، والخبرة، والمسمى الوظيفي".

الفصل الثالث

المنهجية والإجراءات

منهجـــية الدراسة

تعتمد المنهجية المتبعة في هذه الدراسة على المــنهج الوصــفي المســحي الميداني الذي تضمن مسحاً مكتبياً المستند إلى المراجع والمصادر الجــاهزة لبنـــاء الإطار النظري للدراسة، والاستطلاع الميداني لجمع البيانات بوساطة أداة الدراسة، وتحليلها إحصائياً للإجابة عن أسئلة الدراسة، واختبار صحة فرضياتها.

مجتمع الدراسة وعينتها

يتكون مجتمع الدراسة من جميع العاملين في قسم أو وحدة الحاسوب في كــل من وزارة الاتصالات وتكنولوجيا المعلومات، ووزارة الماليـــة، ووزارة الصـــناعة والتجارة، ووزارة التخطيط، وأمانة عمان الكبرى في المملكة الأردنيـــة الهاشـــمية بمختلف مسمياتهم (المبرمج، ومحلل النظم، ومدخل البيانات، والمشـــغل، ومهنـــدس الكمبيوتر، والفني) ويبلغ عددهم(148)مبحوثاً . وقد قامت الباحثـــة بمســـح شـــامل لوزارات مجتمع الدراسة كافة لحصر أعداد مجتمع هذه الدراسة. وســـحبت عينـــة عشوائية بســـيطة مـــنهم بنســـبة(84.5%)، وبـــذلك يكـــون حجـــم العينـــة(125) مفردة.(الملحق رقم 1) ، وقد تم توزيع ما مجموعه (125) استبانـــة ، استرجع منها (115) استبانة بنسبة استرجاع بلغت(92%) و استبعاد(5) استبانات لعدم صلاحيتها للتحليل ، وبذلك خضعت للتحليل(110) اســـتبانة تشـــكل مـــا نســـبته(96%) مـــن الاستبانات المسترجعة وما نسبته(88%) من عينة الدراسة، وما نسبة(74.3 %) من مجتمع الدراسة وهي نسبة مقبولة لأغراض البحث العلمي.

أداة الدراسة

تم تطوير استبانه وبناؤها لقياس أثر التهديدات الأمنية في أمن المعلومات في ضوء تطبيق الحكومة الإلكترونية في عدد من الوزارات الأردنية وأمانـــة عمـــان الكبرى(الملحق رقم 2)، وتتكون هذه الاستبانة من ثلاثة أقسام هي:

القسم الأول: يتضمن المعلومات العامة هي: (الجنس؛ والعمـــر؛ والخبـــرة؛ والمؤهل العلمي؛ والمسمى الوظيفي).

القسم الثاني: يحتوي هذا القسم على(54) فقرة تضم متغيرات الدراســـة ،إذ تقيس الفقرات من(1 - 30) متغير الدراسة المســـتقل؛ وهـــو التهديـــدات الأمنيـــة بمصادرها الداخلية والخارجية، وتقيس الفقرات من(31- 54) متغير الدراسة التابع؛ وهو أمن المعلومات ممثلاً بنتائج التهديدات الأمنية المباشرة وغير المباشرة.

القسم الثالث: يحتوي هذا القسم على(14) فقرة تضم أبعاداً تنظيمية وتقنيـــة وقانونية لأغراض استكشافية، إذ تقيس الفقرات من(1- 5) أبعاداً تنظيمية ومن(6-9) أبعاداً تقنية ومن (10–14) أبعاداً قانونية .

ويوضح الجدول رقم (1) متغيرات الدراسة والفقرات التي تقيس كل متغير .

الجدول رقم (1)

متغيرات الدراسة وأرقام الفقرات التي تقيسها

المتغير	المتغير الفرعي	الفقرات
مصادر التهديدات الداخلية	التقنية	5– 1
	البشرية	13–6
مصادر التهديدات الخارجية	الكوارث الطبيعية	18–14
	المحترفون والقراصنة	24–19
	البرمجيات الخبيثة	30–25
نتائج التهديدات المباشرة	تهديد الأمن المادي	35–31
	تهديد أمن التطبيقات	38–36
	تهديد أمن قواعد البيانات	41–39
	تهديد أمن الشبكات	45–42
نتائج التهديدات غير المباشرة	تهديد الموثوقية	48–46
	تهديد الخصوصية	51–49
	تهديد التكاملية	

وتم صياغة وبناء فقرات هذين المتغيـــرين استرشـــاداً بأدبيـــات موضـــوع الدراسة، وبشكل خـــاص دراســـة (البيـــاتي ،1996) ، وصـــنفت الإجابـــة وفـــق

مقياس(ليكرت الخماسي)، وحددت بخمس إجابات هي (تنطبق دائماً؛ وتنطبق غالباً؛ وتنطبق أحياناً؛ وتنطبق نادراً؛ ولا تنطبق أبداً)، وأعطيت الإجابات أرقاماً من(1-5)، بحيث يدل الرقم(1) على(لا تنطبق أبداً) والرقم(5) على (تنطبق دائماً) .

صدق الأداة وثباتها

للتحقق من مدى صدق محتوى الأداة عرضت على هيئة محكمين أثناء مراحل إعدادها(الملحق رقم 3) وذلك للتأكد من صلاحيتها لأغراض الدراسة.

وجرى الأخذ بملاحظات هيئة التحكيم الواردة . كما تم استخراج معامل الثبات (كرونباخ ألفا) للتأكد من الاتساق الداخلي للفقرات، وقد بلغت قيمته كما يلي :

الجدول رقم (2)

قيمة معامل الثبات (الاتساق الداخلي) لكل متغير من متغيرات الدراسة

رقم المتغير	أرقام الفقرات	اسم المتغير	معامل الثبات (كرونباخ الفا)
1	13-1	التهديدات ألامنية الداخلية	0.7823
2	30-14	التهديدات ألامنية الخارجية	0.8801
3	45-31	نتائج التهديدات المباشرة	0.7881
4	54-46	نتائج التهديدات غير المباشرة	0.8045
4-1	54-1	المتغيرات كافة	0.8976

يلاحظ من الجدول رقم (2) أن معاملات الثبات لجميع متغيرات الدراسة مرتفعة، إذ بلغ معامل الثبات لفقرات الأداة كافة(ألفا =0.8976) وهي نسبة ثبات عالية ومقبولة لأغراض إجراء الدراسة.

المعالجة الإحصائية

للإجابة عن أسئلة الدراسة واختبار صحة فرضياتها، تم استخدام أساليب الإحصاء الوصفي والتحليلي الآتية ، وذلك باستخدام الرزمة الإحصائية(SPSS.10):

1-مقاييس الإحصاء الوصفي (Descriptive Statistic Measures) وذلك لوصف خصائص عينة الدراسة، اعتماداً على التكرارات والنسب المئوية ، ومن

أجل الإجابة عن أسئلة الدراسة ومعرفة الأهمية النسبية باستخدام المتوسطات الحسابية والانحرافات المعيارية .

2-مصفوفة معامل ارتباط (بيرسون) ، للتأكد من أهمية علاقات الارتباط بين أبعاد متغيرات الدراسة المستقلة وأبعاد المتغير التابع .

3- تحليل الانحدار المتعدد (Multiple Regression Analysis) لاختبار فرضيات الدراسة.

التعريفات الإجرائية

وهذا استعراض لأهم التعريفات الإجرائية المتعلق بموضوع الدراسة وهي على النحو التالي :

1-سياسة أمن المعلومات الحكومية(التقليدية):هي مجموعة القواعد والإجراءات التي يطبقها الأفراد لدى تعاملهم مع البيانات والمعلومات داخل المنظمة لإنجاز العمل بشكله اليدوي التقليدي، وترتبط هذه القواعد بشؤون حركة المعلومات دخولا وخروجاً، وإدارة هذه المعلومات وتنظيمها.

2-سياسة أمن المعلومات للحكومة الإلكترونية:هي مجموعة القواعد والإجراءات المتبعة داخل المنظمة من الأفراد لدى تعاملهم مع المعلومات والتقنيات لإنجاز العمل بشكل إلكتروني "مؤتمت" وترتبط هذه القواعد بشؤون حركة المعلومات داخل النظام كمدخلات ومخرجات، والعمل على تنظيمها، وإدارتها، وحمايتها.

3-مصادر التهديدات الأمنية : هي مجموعة الأدوات والمسببات التي يتم بوساطتها تنفيذ التهديد وحدوثه فعلاً، وقد تكون مصادر داخلية أو خارجية. واشتملت هذه الدراسة على المصادر الداخلية متضمنة(التقنية والبشرية) والمصادر الخارجية متضمنة (الكوارث الطبيعية، والمحترفين والقراصنة، والبرمجيات الخبيثة).

4-نتائج التهديدات الأمنية: هي مجموعة الآثار والتأثيرات الناتجة عن مصادر التهديدات على أمن المعلومات، وهذه النتائج منها ما يسهل تلمسها التي تظهر فور حدوث التهديد واعتمدتها هذه الدراسة كنتائج مباشرة متضمنة(تهديد الأمن المادي؛ وتهديد أمن التطبيقات؛ وتهديد أمن القواعد؛ وتهديد أمن الشبكات) ونتائج غير

مباشرة؛ وهي النتائج التي لا يسهل تلمسها فور حدوث التهديد، لكن بعـد حصـول التهديد نستشعر بها ونتلمسها، وتتضمن (تهديد الموثوقية؛ وتهديـد الخصوصـية؛ وتهديد التكاملية).

الفصل الرابع

عرض النتائج

أولاً :وصف خصائص عينة الدراسة.

الجدول رقم (3)

خصائص عينة الدراسة

المتغير	الفئة	العدد	النسبة
الجنس	ذكور	69	%62.7
	إناث	41	%37.3
العمر	29 سنه فأقل	48	%43.6
	30 –39 سنه	36	%32.7
	40–49 سنه	22	%20.0
	50سنه فأكثر	4	%3.6
المؤهل العلمي	الثانوية العامة فما دون	5	%4.5
	الدبلوم المتوسط	21	%19.1
	البكالوريوس	77	%70.0
	الدراسات العليا	7	%6.4
الخبرة	5 سنوات فأقل	45	%40.9
	6–10 سنوات	30	%27.3
	11–15 سنة	21	%19.1
	16 سنة فأكثر	14	%12.7
المسمى الوظيفي	الإداريون	10	%9.1
	المبرمجون	54	%49.1
	الفنيون	28	%25.5
	مدخلو البيانات	18	%16.4

يبين الجدول رقم(3) أن عدد الذكور يشكل غالبية أفراد العينة، إذ بلغت نسبة الذكور (62.7%) بينما بلغت نسبة الإناث(37.3%) وهذا يعكس واقع المؤسسات المبحوثة، إذ تفوق، في الغالب، نسبة الذكور فيها نسبة الإناث .

وفيما يتعلق بمتغير العمر، كانت أعلى نسبة هي الفئة العمرية(29 سنه فأقل) إذ بلغت نسبتها(43.6%) تلتها فئة(30–39 سنه) وبنسبة(32.7%) ثم الفئة الثالثة (40–49 سنه) وبنسبة(20%) وتشكل تلك الفئات الثلاث النسبة الغالبة من العاملين فعلياً في المؤسسات المبحوثة، وكانت أقل فئة من(50 سنه فأكثر) وبلغت نسبتها (3.6%)، ومرد ذلك إلى أن المجتمع الأردني مجتمع فتي ومجتمع الدراسة هم أصحاب تخصص فتي وحديث، وهو تخصص الحاسوب فمن الطبيعي ان تبرز مثل هذه النتائج .

أما فيما يتعلق بمتغير (المؤهل العلمي) فكانت أعلى نسبة هي من حملة شهادة البكالوريوس(70%) تلا ذلك حملة شهادة (الدبلوم المتوسط) إذ بلغت نسبتهم (19.1%)، وأقل النسب كانت تتمثل بحملة الثانوية العامة فما دون، وبلغت نسبتهم (4.5%) كما يشكل حملة(الدراسات العليا) نسبه قليلة اذ بلغ عددهم(7) وبنسبة(6.4%) وهذا مؤشر على ارتفاع نسبة حملة الشهادة الجامعية الأولى من عينة الدراسات في الوزارات الأردنية، وهذا يؤكد حرص الإدارة العليا في الوزارات على توافر التأهيل العلمي المناسب لشاغلي الوظائف .

وحول متغير الخبرة، فقد كانت أعلى نسبة(5 سنوات فأقل) وبلغت(40.9%) وذلك يعكس واقع الأعمال الإلكترونية في المؤسسات الحكومية بعامة والمؤسسات المبحوثة بخاصة، فالخبرات المتوافرة فيها مازالت قليلة في عددها ومحدودة في عمرها الوظيفي، فالصفة الغالبة على العاملين في الوزارات المبحوثة ممن يتخصصون في الأعمال الإلكترونية انهم حديثو التخرج والتعيين، ومن ثم فإنهم لا يمتلكون الخبرة الطويلة، وتأتي فئة 6–10 سنوات) في المرتبة الثانية، وبلغت نسبتهم(27.3%) وتقترب منها فئة(11–15 سنة)، وبلغت نسبتها(19.1%) أما اقل الفئات فهي(16 سنه فأكثر) وبلغت نسبتها(12.7%).

أما فيما يختص بمتغير المسمى الوظيفي، فقد شكل المبرمجون أكبر الفئـــات بنسبة بلغت (49.1%) تلاها فئة الفنيين بنسبة (25.5%) وتأتي بعدها فئة (مــدخلي البيانات) بنسبة(16.4%)، وكانت أقل نسبة ممثلة في الفئة هم (الإداريون) وبلغــت (9.1%) وهذا يعكس واقع متطلبات المرحلة الحالية للحكومــة الإلكترونيــة التــي تتطلب عدداً كبير من (المبرمجين، والمحللين، والفنيين) لتهيئة الــوزارات لتطبيــق الحكومة الإلكترونية .

ثانياً :الإجابة عن أسئلة الدراسة

فيما يلي عرض لنتائج التحليل الإحصائي الوصفي للبيانات، بالاعتماد على المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لمتغيرات الدراسة وفقراتها. وقد استخدم في أداة الدراسة مقياس متدرج يعبر عن إجابات أفراد العينة على النحو التالي:

تنطبق دائماً	تنطبق غالباً	تنطبق أحيانا	نادراً ما تنطبق	لاتنطبق ابداً
5	4	3	2	1

وقد اعتبرت قيمة المتوسطات الحسابية والأهمية النسبية لإجابات أفراد العينة على النحو التالي :

(1−2.49 ضعيفة)، (2.50−3.49 متوسطة)، (3.50−5 عالية).

الإجابة عن سؤال الدراسة الأول الذي ينص على :

"ما هي تصورات المبحوثين لمصادر التهديدات الداخلية لأمن المعلومات في العمل الحكومي"؟

ومن أجل الإجابة عن هذا الســؤال تــم احتســاب المتوســطات الحســابية والانحرافات المعيارية والأهمية النسبية لإجابات أفراد عينة الدراسة عــن فقــرات المتغيرات الفرعية لمصادر التهديدات الداخلية، وعلى النحو التالي:

الجدول رقم (4)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير التهديدات التقنية.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
1	إن نماذج التحكم"المذكرات"المتعلقة بالتشغيل الإلكتروني في منظمتي تعد كافية.	3.6182	0.9480	%72.36	4	مرتفع
2	إن تحديث الأنظمة بعد اكتشاف ثغرات أمنية فيها يتم على الفور	4.1545	0.9661	%83.09	1	مرتفع
3	تستخدم كلمات مرور افتراضية في ربط الأنظمة التي يتم اختيارها بالإنترنت في منظمتي.	3.6909	1.2396	%73.82	3	مرتفع
4	يتم التخلص من المخلفات التقنية(الأقراص والأوراق)الخاصة بالعمل الإلكتروني في المنظمة بصورة مناسبة.	3.5364	1.2317	%70.73	5	مرتفع
5	الوسائل التقنية المستخدمة في حماية أنظمة المعلومات بالمنظمة تعتبر متطورة	4.0182	0.8881	%80.36	2	مرتفع
1-5	المتوسط الحسابي الكلي	3.8036	0.7203	%76.07	-	مرتفع

يتضح من الجدول رقم(4) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بالتهديدات التقنية قد جاء مرتفعاً، بمتوسط حسابي مقداره(3.8036) بأهمية نسبية(76.07%)، وقد جاءت الفقرة رقم(2)(إن هنالك تحديثاً للأنظمة بعد اكتشاف ثغرات أمنية فيها يتم على الفور) في المرتبة الأولى بمتوسط حسابي(4.1545)، وبأهمية نسبية(83.09%)، تلا ذلك الفقرة رقم(5) (الوسائل التقنية المستخدمة في حماية أنظمة المعلومات بالمنظمة تعتبر متطورة) بمتوسط حسابي(4.0182) وبأهمية نسبية(80.36%)، في حين جاء في المرتبة الثالثة الفقرة رقم(3)(تستخدم كلمات مرور افتراضية في ربط الأنظمة التي يتم اختيارها بالإنترنت في منظمتي) بمتوسط حسابي (3.6909) وبأهمية نسبية (73.82%)، وأخيراً جاءت الفقرة رقم (4)(يتم التخلص من المخلفات التقنية(الأقراص والأوراق)الخاصة بالعمل الإلكتروني

في المنظمة بصورة مناسبة)في المرتبة الأخيرة بمتوسط حسابي(3.5364) وبأهمية نسبية (70.73%) .

وتتوافق هذه النتائج مع واقع العمل الإلكتروني في الوزارات مجتمع الدراسة، فهو عمل في مراحله الأولى يحرص فيه على استخدام وسائل تقنية حديثة ومواكبة التطورات لتحديث الأنظمة بصوره مستمرة لتفادي الثغرات الأمنية ومواجهتها .

الجدول رقم (5)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير التهديدات البشرية .

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
6	يسمح بتداول كلمات السر بين الموظفين عبر الهاتف في منظمتي	2.7818	1.1916	%55.64	8	متوسط
7	إن العاملين في مجال المعلوماتية بالمنظمة يمتلكون مؤهلات تقنية جيدة	3.8818	0.7750	%77.64	2	مرتفع
8	إن العاملين في مجال المعلوماتية بالمنظمة يمتلكون خبرات جيدة.	3.7909	0.8025	%75.82	3	مرتفع
9	يخضع العاملون في مجال الأعمال الإلكترونية بالمنظمة لبرامج تدريبية بصورة مستمرة	3.6273	1.0654	%72.55	4	مرتفع
10	يخضع العاملون في الأعمال الإلكترونية بالمنظمة لعملية استقطاب وانتقاء محكمة.	3.0364	0.9571	%60.73	7	متوسط
11	يتوافر في المنظمة نظم لضبط ومراقبة تحركات العاملين.	3.5182	1.1710	%70.36	5	مرتفع
12	يتوافر في منظمتي رقابة على البريد الصادر والوارد الخاص بالعاملين	3.2636	1.2970	%65.27	6	متوسط
13	تستخدم المنظمة إجراءات محددة في السماح للوصول إلى المعدات الإلكترونية والبرمجيات.	4.0909	0.8835	%81.82	1	مرتفع
6–13	المتوسط الحسابي الكلي	3.4989	0.5337	%69.98	-	متوسط

يتضح من الجدول رقم(5) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بالتهديدات البشرية قد جاء متوسطاً، بمتوسط حسابي مقداره(3.4989) بأهمية نسبية(69.98%)، وقد جاءت الفقرة رقم(13)(تستخدم المنظمة إجراءات محددة في السماح للوصول إلى المعدات الإلكترونية والبرمجيات) في المرتبة الأولى بمتوسط حسابي(4.0909)، وبأهمية نسبية(81.82%)، تلا ذلك الفقرة رقم(7) (إن العاملين في مجال المعلوماتية بالمنظمة يمتلكون مؤهلات تقنية جيدة) بمتوسط حسابي(3.7909) وبأهمية نسبية(75.82%)، في حين جاء في المرتبة الثالثة الفقرة رقم (8) (إن العاملين في مجال المعلوماتية بالمنظمة يمتلكون خبرات جيدة) بمتوسط حسابي(3.7909) وبأهمية نسبية(75.82%)، وأخيراً جاءت الفقرة رقم(6)(يسمح بتداول كلمات السر بين الموظفين عبر الهاتف في منظمتي) في المرتبة الأخيرة بمتوسط حسابي(2.7818) وبأهمية نسبية (55.64%).

ويشير ذلك إلى تقيد أفراد العينة بالإجراءات المحددة في وزاراتهم، والى اهتمامهم بضرورة امتلاك العاملين مؤهلات وخبرات تقنية ، وتتفق نتائج الإجابة على سؤال الدراسة الأول مع نتائج دراسة (أبو موسى ،2002) التي ركزت على دراسة طرق التحكم المطبقة لمنع الثغرات الأمنية وكشفها، ودراسة(العوامله،2002) التي توصلت إلى ضرورة توافر الخبرة والتأهيل العلمي والتقني لدى العنصر البشري بوصفها متطلبات لنجاح تطبيق الحكومة الإلكترونية ، وتختلف مع نتائج دراسة (Detmar w,1996) التي توصلت إلى أهمية استخدام نماذج التحكم والتخطيط الأمني في تحليل الخطر والتهديدات .

الإجابة عن سؤال الدراسة الثاني الذي ينص على :

"ما هي تصورات المبحوثين لمصادر التهديدات الخارجية لأمن المعلومات في العمل الحكومي"؟

ومن أجل الإجابة عن هذا السؤال تم احتساب المتوسطات الحسابية والانحرافات المعيارية والأهمية النسبية لإجابات أفراد عينة الدراسة عن فقرات المتغيرات الفرعية لمصادر التهديدات الخارجية، وعلى النحو التالي:

الجدول رقم (6)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير الكوارث الطبيعية.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة المتوسط
14	تستخدم المنظمة في منظوماتها الإلكترونية وسائل حماية من الكوارث الطبيعية	3.3364	1.2137	%66.73	4	متوسط
15	توجد وسائل بديلة لتقديم الخدمة الإلكترونية في حال التعرض إلى كارثة طبيعية.	3.0545	1.1874	%61.09	5	متوسط
16	يتم الاحتفاظ بنسخ إضافية من البرامج الإلكترونية توضع في أماكن آمنة.	4.4818	0.8321	%89.64	1	مرتفع
17	توجد خطط طوارئ خاصة بالعمل الإلكتروني في المنظمة في حال حصول كارثة طبيعية.	3.3727	1.2256	%67.45	3	متوسط
18	العمل الإلكتروني في المنظمة ليس عرضة للكوارث الطبيعية بصورة مستمرة.	3.4727	1.2169	%69.45	2	متوسط
18-14	المتوسط الحسابي الكلي	3.5436	0.7858	%70.87	-	مرتفع

يتضح من الجدول رقم(6) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق(بالكوارث الطبيعية)قد جاء مرتفعاً، إذ بلغ(3.5436) وقد تراوحت المتوسطات الحسابية لفقراته بين(4.4818) و(3.0545) بأهمية نسبية (70.87%)، وقد جاءت الفقرة رقم(16)(يتم الاحتفاظ بنسخ إضافية من البرامج الإلكترونية توضع في أماكن آمنة) في المرتبة الأولى بمتوسط حسابي(4.4818)، وبأهمية نسبية(89.64%)، تلا ذلك الفقرة رقم(18)(العمل الإلكتروني في المنظمة ليس عرضة للكوارث الطبيعية بصورة مستمرة) وبمتوسط حسابي (3.4728) وبأهمية نسبية(69.45%)، في حين جاء في المرتبة الثالثة الفقرة رقم(17) (توجد خطط طوارئ خاصة بالعمل الإلكتروني في المنظمة في حال حصول كارثة طبيعية) بمتوسط حسابي(3.3727) وبأهمية نسبية(67.45%) ، وأخيراً جاءت الفقرة

يتضح من الجدول رقم (8) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بالبرمجيات الخبيثة قد جاء مرتفعاً، بمتوسط حسابي مقداره(3.7985) بأهمية نسبية (75.97%)، وقد جاءت الفقرة رقم (26) (تستخدم في المنظمة برمجيات مضادة للفيروسات) في المرتبة الأولى بمتوسط حسابي (4.5909)، وبأهمية نسبية (91.82%)، تلا ذلك الفقرة رقم (25) (يتم التأكد من سلامة المعدات الإلكترونية والبرامج المشتراة قبل استخدامها) بمتوسط حسابي (4.5000) وبأهمية نسبية (90%)، في حين جاء في المرتبة الثالثة الفقرة رقم (27) (تعتمد المنظمة على إجراءات سيطرة للحيلولة دون الوصول إلى برمجياتها مثل (أجهزة إنذار مفاتيح) بمتوسط حسابي (3.8455) وبأهمية نسبية (76.91%)، وأخيراً جاءت الفقرة رقم (29) (إجراءات الحماية للعمل الإلكتروني بالمنظمة تحول دون تهديد البرامج الخبيثة) في المرتبة الأخيرة بمتوسط حسابي (3.1273) وبأهمية نسبية (62.55%).

وبملاحظة نتائج فقرات هذا المتغير يتبين أن هناك ارتفاعاً في مستوى الفقرات ذوات الأرقام (25، 26، 27) التي تعبر عن ضرورة حرص المنظمة على الوقاية ضد البرمجيات الخبيثة، وأهمية استخدام وسائل متطورة تواكب ظهور الجديد من الفيروسات والبرمجيات الخبيثة.

وتتفق نتائج الإجابة عن سؤال الدراسة الثاني مع نتائج دراسة (البياتي ،1996) الذي توصل إلى أن الفيروسات ليست أخطر التهديدات ، لأن المنظمة تستخدم معدات مضادة للفيروسات ودراسة (Chen & Gart ,2001) التي توصلت إلى أهمية تقييم البرمجيات بوصفها عنصراً أساسياً لنجاح تطبيق الحكومة الإلكترونية.

الإجابة عن سؤال الدراسة الثالث الذي ينص على :

"ما هي تصورات المبحوثين للنتائج المباشرة لتهديدات أمن المعلومات"؟

ومن أجل الإجابة عن هذا السؤال تم احتساب المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد عينة الدراسة عن فقرات المتغيرات الفرعية للنتائج المباشرة لأمن المعلومات، وعلى النحو التالي:

رقم(15) (توجد وسائل بديلة لتقديم الخدمة الإلكترونية في حال التعرض إلى كارثة طبيعية) في المرتبة الأخيرة بمتوسط حسابي(3.0545) وبأهمية نسبية(61.09%).

يؤكد مضمون هذه الفقرات على أن الخطر الحقيقي عند حدوث كارثة طبيعية يتجلى في عدم الاحتفاظ بنسخ إضافية واحتياطية من البرامج الإلكترونية في مكان آمن.

الجدول رقم (7)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير المحترفين والقراصنة.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
19	تعتبر وسائل الحماية المطبقة في المنظمة ضد السرقات مناسبة	3.6818	1.0131	%73.64	3	مرتفع
20	تستخدم المنظمة نظاماً للتشفير أثناء نقل البيانات	3.4273	1.3711	%68.55	5	متوسط
21	يتم اعتماد إجراءات سيطرة لمنع المتطفلين أو كشفهم في حال دخولهم على الشبكات.	3.4182	1.2735	%68.36	6	متوسط
22	يتم تغيير كلمات السر والشيفرات بشكل دوري.	4.1909	0.9530	%83.82	1	مرتفع
23	تتعامل المنظمة بحرص أكبر مع المستفيد (الخارجي) صاحب الخبرة التقنية.	3.6364	1.0898	%72.73	4	مرتفع
24	تتم مراقبة تحركات عمال الصيانة الإلكترونية الخارجيين.	3.9909	0.9814	%79.82	2	مرتفع
19-24	المتوسط الحسابي الكلي	3.7242	0.7366	%73.64	-	مرتفع

يتضح من الجدول رقم (7) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بالمحترفين والقراصنة قد جاء مرتفعاً، إذ بلغ (3.7242) بأهمية نسبية (73.64%)، وقد جاءت الفقرة رقم (22) (يتم تغيير كلمات السر والشيفرات بشكل دوري) في المرتبة الأولى بمتوسط حسابي (4.1909)، وبأهمية نسبية(83.82%)، تلا ذلك الفقرة رقم (24) (تتم مراقبة تحركات عمال الصيانة الإلكترونية الخارجيين)

بمتوسط حسابي (3.9909) وبأهمية نسبية (79.82%)، في حين جاء في المرتبة الثالثة الفقرة رقم (19) (تعتبر وسائل الحماية المطبقة في المنظمة ضد السرقات مناسبة) بمتوسط حسابي (3.6818) وبأهمية نسبية (73.64%)، وأخيراً جاءت الفقرة رقم (21) (يتم اعتماد إجراءات سيطرة لمنع المتطفلين أو كشفهم في حال دخولهم على الشبكات) في المرتبة الأخيرة بمتوسط حسابي (3.4182) وبأهمية نسبية (68.36%).

ويشير ذلك إلى أهمية تغيير كلمات السر والشيفرات بشكل دوري بوصفها وسيلة احتياطية ووقائية ضد الهجمات الخارجية، وكذلك ضرورة الحرص في التعامل مع عمال الصيانة الخارجيين ،وضبط تحركاتهم، ومراقبتهم داخل المنظمة .

الجدول رقم (8)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير البرمجيات الخبيثة.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
25	يتم التأكد من سلامة المعدات الإلكترونية والبرامج المشتراة قبل استخدامها.	4.5000	0.7263	%90.00	2	مرتفع
26	تستخدم في المنظمة برمجيات مضادة للفيروسات	4.5909	0.6813	%91.82	1	مرتفع
27	تعتمد المنظمة على إجراءات سيطرة للحيلولة دون الوصول إلى برمجياتها مثل (أجهزة إنذار، مفاتيح)	3.8455	1.0937	%76.91	3	مرتفع
28	يدرب العاملون بشكل مستمر على كيفية التعامل مع البرمجيات الخبيثة	3.2909	1.1990	%65.82	5	متوسط
29	إجراءات الحماية للعمل الإلكتروني بالمنظمة تحول دون تهديد البرامج الخبيثة	3.1273	1.2349	%62.55	6	متوسط
30	تتم توعية العاملين باستمرار حول الأساليب المتبعة لمواجهة تهديد البرمجيات الخبيثة.	3.4364	1.2156	%68.73	4	متوسط
25-30	المتوسط الحسابي الكلي	3.7985	0.7115	%75.97	-	مرتفع

الجدول رقم (9)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير تهديد الأمن المادي.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
31	تكثر الأعطال والتوقفات في الحاسوب الرئيسي Mainframe للمنظمة	3.1091	1.0258	%62.18	5	متوسط
32	إن حداثة الأجهزة والمعدات الإلكترونية المستخدمة لا تمنع حدوث أعطال وتوقفات متكررة.	3.5000	0.9838	%70.00	1	مرتفع
33	تتصف الأضرار التقنية التي تتعرض لها المكونات المادية الإلكترونية بأنها بالغة.	3.3273	1.1423	%66.55	2	متوسط
34	يعد موقع مبنى الحاسوب الرئيسي هو السبب في تعرضه للعديد من التهديدات	3.0818	1.1181	%61.64	4	متوسط
35	تعتبر إجراءات تأمين الأجهزة المادية من (حاسبات وطابعات) غير ملائمة	3.1818	1.0852	%63.64	3	متوسط
35-31	المتوسط الحسابي الكلي	3.2400	0.9454	%64.80	-	متوسط

يتضح من الجدول رقم (9) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بتهديد الأمن المادي قد جاء متوسطاً، بمتوسط حسابي مقداره (3.2400) بأهمية نسبية (%64.80)، وقد جاءت الفقرة رقم (32) (إن حداثة الأجهزة والمعدات الإلكترونية المستخدمة لا تمنع حدوث أعطال وتوقفات متكررة) في المرتبة الأولى بمتوسط حسابي (3.5000)، وبأهمية نسبية (%70)، تلا ذلك الفقرة رقم (33) (تتصف الأضرار التقنية التي تتعرض لها المكونات المادية الإلكترونية بأنها بالغة) بمتوسط حسابي (3.3273) وبأهمية نسبية (%66.55)، في حين جاء في المرتبة الثالثة الفقرة رقم (35) (تعتبر إجراءات تأمين الأجهزة المادية من (حاسبات وطابعات) غير ملائمة بمتوسط حسابي (3.1818) وبأهمية نسبية (%63.64)،

وأخيراً جاءت الفقرة رقم (31)(تكثر الأعطال والتوقفات في الحاسوب الرئيسي Mainframe للمنظمة) في المرتبة الأخيرة بمتوسط حسابي (3.1091) وبأهمية نسبية (62.18%).

وهذا يؤكد على أن الأجهزة والمعدات الحديثة وحدها لا تكفي لتوفير حماية مادية لأنظمة الحاسوب، إذ لابد من وسائل مساندة فنية وغير فنية ترافق هذه الأجهزة وكذلك لابد من رقابه من الإدارة العليا .

الجدول رقم (10)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير تهديد أمن التطبيقات.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
36	تتعرض البرمجيات التطبيقية إلى تهديد خارجي أو / وداخلي من حين لآخر.	3.2091	1.2123	%64.18	3	متوسط
37	على الرغم من حزم الأمان المستخدمة لتأمين البرمجيات والتطبيقات، فإنها عرضه لتهديدات المستمرة.	3.3182	1.0746	%66.36	2	متوسط
38	اختلاف بيئة عمل المنظمة ليس له أثر على سلامة نظم التشغيل المستخدمة.	3.4091	1.0431	%68.18	1	متوسط
36-38	المتوسط الحسابي الكلي	3.3121	0.9926	%66.24	-	متوسط

يتضح من الجدول رقم(10) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بأمن التطبيقات قد جاء متوسطاً، بمتوسط حسابي مقداره(3.3121) بأهمية نسبية(66.24%)، وقد جاءت الفقرة رقم (38) (اختلاف بيئة عمل المنظمة ليس له أثر على سلامة نظم التشغيل المستخدمة) في المرتبة الأولى بمتوسط حسابي (3.3121)، وبأهمية نسبية (66.24%)، تلا ذلك الفقرة رقم (37) (على الرغم من حزم الأمان المستخدمة لتأمين البرمجيات والتطبيقات، فإنها عرضة لتهديدات المستمرة) بمتوسط حسابي(3.3182)وبأهمية نسبية(66.36%)،وأخيراً جاءت الفقرة

رقم(36) (تتعرض البرمجيات التطبيقية إلى تهديد خارجي أو/وداخلي من حين لآخر)في المرتبة الأخيرة بمتوسط حسابي(3.2091)وبأهمية نسبية(64.18%).

وتعد هذه النتائج متوقعه في الوزارات مجتمع الدراسة بسبب عدم تغطية العمل الإلكتروني بشكل كامل، فهو جزئي، وبالتالي تعرضه للتهديدات أيضا في مراحله البدائية وخطواته الأولى، كما تشير الفقرة(37) إلى أن هنالك تهديدات مستمرة على البرمجيات والتطبيقات رغم استخدام أجهزة أمان، وهذا أمر طبيعي لأن حزم الأمان المستخدمة هي عن تهديد معروف ومحدد، ولكن التهديد الجديد يحتاج إلى وسيلة أمان جديدة تناسبه، ومن ثم فإن هذه حاله مستمرة، فكل تهديد جديد بحاجة إلى وسائل وأجهزة أمان جديدة تناسبه .

الجدول رقم (11)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير تهديد أمن قواعد البيانات.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
39	إن معظم التهديدات لقواعد بيانات المنظمة هو من أفراد غير متخصصين.	3.3455	1.1287	%66.91	2	متوسط
40	إن عدم تحديد الفئات المستخدمة لقواعد بيانات المنظمة يجعلها عرضة للتهديد.	3.4909	1.0815	%69.82	1	متوسط
41	تفتقد إدارة قواعد البيانات إلى خطة لتأمين البيانات	3.1636	1.1456	%63.27	3	متوسط
39-41	المتوسط الحسابي الكلي	3.3333	1.0187	%66.67	-	متوسط

يتضح من الجدول رقم(11) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بأمن قواعد البيانات قد جاء متوسطاً، بمتوسط حسابي مقداره (3.3333) بأهمية نسبية(66.67%)، وقد جاءت الفقرة رقم(40) (إن عدم تحديد الفئات المستخدمة لقواعد بيانات المنظمة يجعلها عرضة للتهديد) في المرتبة الأولى بمتوسط حسابي (3.4909)، وبأهمية نسبية(69.82%)، تلا ذلك الفقرة رقم (39)

(إن معظم التهديدات لقواعد بيانات المنظمة هو من أفراد غير متخصصين) بمتوسط حسابي(3.3455) وبأهمية نسبية(66.91%)، وأخيراً جاءت الفقرة رقم (41) (تفتقد إدارة قواعد البيانات إلى خطة لتأمين البيانات) في المرتبة الأخيرة بمتوسط حسابي (3.1636) وبأهمية نسبية (63.27%).

وهذا مؤشر على أن الخطر الحقيقي الذي يهدد أمن قواعد البيانات يكمن في محتوى الفقرات (39,40) إذ إن استخدام قواعد البيانات من غير المتخصصين وعدم تحديد فئات المستخدمين لقواعد البيانات يشكل خطراً وتهديداً لأمنية قواعد البيانات ، أما عن مضمون الفقرة (41) وحصولها على اقل أهمية نسبية ؛ فهذا يخالف دراسة (البياتي ، 1996) ودراسة (Detmar w,1996)، إذ أكد كل منهما أهمية وجود سياسة وخطه أمنية في كل منظمة .

الجدول رقم (12)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير تهديد أمن الشبكات.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
42	إن المشكلات في أنظمة تشغيل الشبكة أو الأنظمة المساندة تؤدي إلى تهديد أمن الشبكة المحلية.	3.4545	1.0461	%69.09	2	متوسط
43	أن نوع الشبكات المستخدمة يقود إلى حدوث أعطال ذات طبيعة تقنية.	3.5455	0.8741	%70.91	1	مرتفع
44	تؤدي الأخطاء البشرية إلى حدوث أعطال في أجزاء الشبكة.	3.1909	1.1691	%63.82	4	متوسط
45	تفتقد الشبكات المحلية إلى وسائل مادية كافية لتأمينها.	3.2455	1.1267	%64.91	3	متوسط
45-42	المتوسط الحسابي الكلي	3.3591	0.8637	%67.18	-	متوسط

يتضح من الجدول رقم (12) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بأمن الشبكات قد جاء متوسطاً، بمتوسط حسابي مقداره (3.3591) بأهمية

نسبية (67.18%) ، وقد جاءت الفقرة رقم (43) (أن نوع الشبكات المستخدمة يقود إلى حدوث أعطال ذات طبيعة تقنية) في المرتبة الأولى بمتوسط حسابي (3.5455)، وبأهمية نسبية (70.91%)، تلا ذلك الفقرة رقم (42) (إن المشكلات في أنظمة تشغيل الشبكة أو الأنظمة المساندة تؤدي إلى تهديد أمن الشبكة المحلية) بمتوسط حسابي (3.4545) وبأهمية نسبية (69.09%)، في حين جاء في المرتبة الثالثة الفقرة رقم (45) (تفتقد الشبكات المحلية إلى وسائل مادية كافية لتأمينها) بمتوسط حسابي (3.2455) وبأهمية نسبية (64.91%)، وأخيراً جاءت الفقرة رقم (44) (تؤدي الأخطاء البشرية إلى حدوث أعطال في أجزاء الشبكة) في المرتبة الأخيرة بمتوسط حسابي (3.1909) وبأهمية نسبية (64.91%).

وهنا يؤكد أفراد العينة أن نوع الشبكات والمشكلات التي تعاني منها الأنظمة المساندة هي وراء أغلب التهديدات التي تقع على الشبكات وأمنها، وأنها تهديدات ذات طابع تقني وليس بشري، كما تؤكد نتائج الإجابة عن الفقرة (44) على عدم إخلاء طرف العنصر البشري من هذا التهديد، والعمل جارٍ في الوزارات الأردنية مجتمع الدراسة على تحديث الشبكات، إذ تعتبر هذه الخطوة من المراحل الأولى للتحول نحو الحكومة الإلكترونية التي تم على الأغلب تخطيها.

وتتفق نتائج الإجابة عن سؤال الدراسة الثالث مع نتائج دراسة (KanKan Halli & Others,2003) ودراسة (الشواف والزلزلة، 1999) وكذلك دراسة (Salem,2003) حيث أكدوا أن عدم تحديد الجهات والفئات المستخدمة والمسؤولة عن النظام المعلوماتي يؤدي إلى حدوث تهديدات ومخاطر أمنية ، كما أكدوا ضرورة وجود جهود قانونية رادعة تساعد في تعزيز الفاعلية الأمنية لنظام المعلومات

الإجابة عن سؤال الدراسة الرابع الذي ينص على :

"ما هي تصورات المبحوثين للنتائج غير المباشرة لتهديدات أمن المعلومات"؟

ومن أجل الإجابة عن هذا السؤال تم احتساب المتوسطات الحسابية ، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد عينة الدراسة عن فقرات المتغيرات الفرعية للنتائج غير المباشرة لأمن المعلومات، وعلى النحو التالي:

الجدول رقم (13)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير تهديد الموثوقية.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
46	تتوافر الموثوقية في العمل الإلكتروني للمنظمة.	3.6091	0.9296	%72.18	1	مرتفع
47	لا تتعرض مصداقية المعلومات المتوافرة إلى الاعتداء.	3.5545	1.0099	%71.09	2	مرتفع
48	تعتبر المعلومات الخاصة بالعمل غير متاحة بين جميع المخولين.	3.4818	1.0729	%69.64	3	متوسط
48-46	المتوسط الحسابي الكلي	3.5485	0.9160	%70.97	-	مرتفع

يتضح من الجدول رقم (13) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بتهديد الموثوقية قد جاء مرتفعاً، بمتوسط حسابي مقداره (3.5485) بأهمية نسبية (70.97%)، وقد جاءت الفقرة رقم (46) (تتوافر الموثوقية في العمل الإلكتروني للمنظمة) في المرتبة الأولى بمتوسط حسابي (3.6091)، وبأهمية نسبية(72.18%)، تلا ذلك الفقرة رقم (47) (لا تتعرض مصداقية المعلومات المتوافرة إلى الاعتداء) بمتوسط حسابي(3.5545) وبأهمية نسبية(71.09%)، وأخيراً جاءت الفقرة رقم (48) (تعتبر المعلومات الخاصة بالعمل غير متاحة بين جميع المخولين) في المرتبة الأخيرة بمتوسط حسابي (3.4818) وبأهمية نسبية (69.64%).

وتعبر هذه النتائج عن حرص أفراد العينة على وصف عملهم وأدائهم بالمصداقية، والموثوقية، والمحافظة على السرية، واعتبارهم العمل والمعلومات المرتبطة به أمانة هم المسؤولون عنها مع ضرورة المحافظة على أسرار العمل الخاصة بالعمل وبالمواطن نفسه .

الجدول رقم (14)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير تهديد الخصوصية.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
49	يشكو المتعاملون مع المنظمة بانتهاك مبدأ الخصوصية.	3.2182	1.1839	%64.36	3	متوسط
50	يعتبر كشف الأرقام السرية والتنصت من أبرز ما يهدد الخصوصية في المنظمة.	3.3909	1.0588	%67.82	2	متوسط
51	تفتقد المنظمة إلى سياسة واضحة ومحددة لحماية الخصوصية.	3.4000	1.0853	%68.00	1	متوسط
49-51	المتوسط الحسابي الكلي	3.3364	1.0182	%66.73	-	متوسط

يتضح من الجدول رقم (14) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بتهديد الخصوصية قد جاء متوسطاً، بمتوسط حسابي مقداره(3.3364) بأهمية نسبية(66.73%)، وقد جاءت الفقرة رقم(51) (تفتقد المنظمة إلى سياسة واضحة ومحددة لحماية الخصوصية)في المرتبة الأولى بمتوسط حسابي(3.4000)، وبأهمية نسبية(68%)، تلا ذلك الفقرة رقم (50) (يعتبر كشف الأرقام السرية والتنصت من أبرز ما يهدد الخصوصية) في المنظمة بمتوسط حسابي(3.3909) وبأهمية نسبيه (67.82%)، وأخيراً جاءت الفقرة رقم(49) (يشكو المتعاملون مع المنظمة بانتهاك مبدأ الخصوصية) في المرتبة الأخيرة بمتوسط حسابي(3.2182) وبأهمية نسبيه(64.36%) .

ولعل هذا يتوافق مع المرحلة الحالية لتطبيق الحكومة الإلكترونية في الأردن في الوزارات مجتمع الدراسة، فالعمل الحكومي حالياً هو خليط من العمل اليدوي والإلكتروني، ومن الطبيعي أن المواطن لم يشكو من انتهاك مبدأ الخصوصية حالياً.

الجدول رقم (15)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية لإجابات أفراد العينة عن فقرات متغير تهديد التكاملية.

رقم الفقرة	محتوى الفقرة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية(%)	الترتيب حسب الأهمية النسبية	المستوى بالنسبة للمتوسط
52	تعمل جميع البرامج بشكل يؤدي إلى سلامة المعلومات.	3.6545	0.9715	%73.09	1	مرتفع
53	أن السياسة الأمنية التي تطبقها المنظمة تقود إلى تحقيق التكاملية.	3.6000	1.0064	%72.00	2	مرتفع
54	لا يتعرض محتوى المعلومات إلى التعديل نتيجة التدخل غير المشروع في المنظمة.	3.3000	1.1538	%66.00	3	متوسط
52-54	المتوسط الحسابي الكلي	3.5182	0.9294	%70.36	-	مرتفع

يتضح من الجدول رقم(15) أن المتوسط الحسابي الكلي لفقرات هذا المتغير المتعلق بتهديد التكاملية قد جاء مرتفعاً، بمتوسط حسابي مقداره(3.5182) بأهمية نسبية(70.36%)، وقد جاءت الفقرة رقم(52) (تعمل جميع البرامج بشكل يؤدي إلى سلامة المعلومات) في المرتبة الأولى بمتوسط حسابي(3.6545)، وبأهمية نسبية (73.09%)، تلا ذلك الفقرة رقم (53) (أن السياسة الأمنية التي تطبقها المنظمة تقود إلى تحقيق التكاملية) بمتوسط حسابي(3.6000) وبأهمية نسبية(72%)، وأخيراً جاءت الفقرة رقم(54) (لا يتعرض محتوى المعلومات إلى التعديل نتيجة التدخل غير المشروع في المنظمة) في المرتبة الأخيرة بمتوسط حسابي (3.3000) وبأهمية نسبية (66%).

وتعكس هذه النتائج حقيقة أن الحكومة الإلكترونية هي في مرحلة تجريبية ومطبقة على عدد من الوزارات ، ضمن ما يسمى بالشبكة الآمنة، وهي التي تشكل مجتمع الدراسة، لم تتعرض فيها تكاملية محتوى المعلومات بعد إلى تهديد واضح ومباشر، إذ أن العمل الإلكتروني الشامل والمتكامل مازال في بداية الطريق .

وتتفـــق نتـــائج الإجابـــة عـــن ســـؤال الدراســـة الرابـــع مـــع دراســـة (دونك وديفينودين ، 1996) ودراسة(Layne & Lee ,2001) وكذلـــك دراســـة (Beheruz&Cynthiac,1990)حيث أكدوا جميعهم على أهميـــة تـــوافر سياســـة خاصة بكل منظمة تحمي السرية، الموثوقية، الخصوصية، وأكدوا دورها في إنجاح الحكومة الإلكترونية.

الإجابة عن سؤال الدراسة الخامس الذي ينص على :

"ما هي طبيعة العلاقة بين متغيرات الدراسة المستقلة والتابعة"؟

ومن أجل الإجابة عن هذا السؤال تم استخدام معامل ارتباط (بيرسون) لتحديد علاقات الارتباط بين المتغيرات المستقلة والمتغير التابع، وكانت النتائج كالتالي :

الجدول رقم (16)

مصفوفة معاملات الارتباط بين مصادر (التهديدات الداخلية والخارجية) والنتائج المباشرة وغير المباشرة لهذه التهديدات الأمنية .

المتغيرات المستقلة / المتغير التابع		تهديدات داخلية		التهديدات الخارجية		
		التهديدات التقنية	التهديدات البشرية	الكوارث الطبيعية	المحترفون والقراصنة	البرمجيات الخبيثة
النتائج المباشرة للتهديدات	الأمن المادي	*0.466	*0.346	*0.452	0.150	*0.361
	أمن التطبيقات	*0.536	*0.434	*0.426	**0.212	*0.432
	أمن قواعد البيانات	*0.473	*0.396	*0.403	0.182	*0.328
	أمن الشبكات	*0.510	*0.317	*0.405	**0.218	*0.271
	النتـــائج المباشـــرة للتهديدات	*0.533	*0.404	*0.453	**0.204	*0.377
النتائج غير المباشرة للتهديدات	الموثوقية	*0.627	*0.382	*0.427	*0.318	*0.413
	الخصوصية	*0.520	*0.413	*0.359	0.158	*0.359
	التكاملية	*0.609	*0.351	*0.417	*0.344	*0.503
	النتـــائج غيـــر المباشرة للتهديدات	*0.635	*0.417	*0.435	*0.290	*0.460

*ذات دلالة إحصائية عند(α=0.01)

**ذات دلالة إحصائية عند(α=0.05)

يتبين من الجدول رقم(16) أن التهديدات التقنية ترتبط ارتباطاً موجباً بالنتـــائج المباشرة للتهديدات، وقد بلغ معامل الارتباط (0.533) وهو ذات دلالـــة إحصـــائية

عند(α=0.01) مقابل ارتباط موجب للتهديدات التقنية بالنتائج غير المباشرة بلغ معامله (0.635)، وهذا يعني أن التهديدات التقنية تسبب اتجاهات إيجابية في النتائج المباشرة وغير المباشرة.

وبالنظر إلى النتائج الإحصائية المبينة في الجدول ذاته، يظهر أن ارتباط التهديدات التقنية بأمن التطبيقات بالنسبة للنتائج المباشرة للتهديدات بشكل أقوى ارتباط، وبلغت قيمته الارتباط(0.536) في حين أن أضعف العلاقات التي ربطت التهديدات التقنية بالنتائج المباشرة هي مع الأمن المادي، وبلغت قيمة معامل الارتباط (0.466). وفيما يتعلق بالنتائج غير المباشرة، فقد كانت أعلى قيمة معامل ارتباط لها مع الموثوقية (0.627) مقابل ارتباطها مع الخصوصية بمعامل بلغت قيمته(0.520)، وهذا مؤشر على أن التهديد الداخلي الحقيقي والأكثر تأثيراً في الوزارات الأردنية المطبقة للحكومة الإلكترونية تحديداً والمرتبطة بالشبكة الآمنة هو التهديد التقني مما يؤكد أن التهديد الحالي في المراحل الأولى هو تهديد مرتبط بالتقنية، وهو مؤشر واقعي .

أما فيما يتعلق بالتهديدات البشرية؛ فإنها ترتبط ارتباطاً موجباً بالنتائج المباشرة، وقد بلغ معاملة (0.404) وهو ذو دلالة إحصائية عند(α=0.01) مقابل ارتباط موجب للتهديدات البشرية بالنتائج غير المباشرة بلغ معامله (0.417)، وهذا يعني أن التهديدات البشرية تسبب اتجاهات إيجابية في النتائج المباشرة وغير المباشرة .

وبالنظر إلى النتائج الإحصائية المبينة في الجدول ذاته، يظهر أن ارتباط التهديدات البشرية بأمن التطبيقات بالنسبة للنتائج المباشرة تشكل أقوى ارتباط وبلغت قيمة معاملة (0.434) في حين أن أضعف العلاقات التي ربطت التهديدات البشرية بالنتائج المباشرة هي مع أمن الشبكات، وبلغت قيمة معاملة (0.317).

وبالنسبة للنتائج غير المباشرة، فقد كانت أعلى قيمة معامل ارتباط للتهديدات البشرية مع الخصوصية(0.413) مقابل ارتباطها مع التكاملية بمعامل بلغت قيمته(0.351)، وهذا مؤشر على أن التهديد البشري، بوصفه تهديداً داخلياً، لم يظهر أي نشاط بعد لأن دوره في هذه المرحلة لم يتبلور بعد هذا من ناحية ، بالإضافة إلى

ان العنصر البشري يتعامل بدرجه أكبر مع البرمجيات؛ أي يهدد أمن التطبيقات، وذلك مؤشر على تقيد العنصر البشري بالتعليمات والإجراءات الأمنية، وجاءت هذه النتيجة عكس ما توصلت له دراسة (البياتي ، 1996) حيث كانت مصادر التهديد الداخلية الناتجة عن العنصر البشري من أكثر مصادر التهديد تأثيراً، إذ تراوحت نسبة تأثيرها بين(70-80%) .

ويتبين من الجدول رقم(16) أن تهديد الكوارث الطبيعية يرتبط ارتباطاً موجباً بالنتائج المباشرة، وقد بلغ معاملة(0.453)هو ذو دلالة إحصائية عند (α=0.01) مقابل ارتباط موجب للكوارث الطبيعية للنتائج غير المباشرة بلغ معامله (0.435)، وهذا يعني أن الكوارث الطبيعية تسبب اتجاهات إيجابية في النتائج المباشرة وغير المباشرة للتهديدات الأمنية .

وبالنظر إلى النتائج الإحصائية المبينة في الجدول ذاته، يظهر أن ارتباط الكوارث الطبيعية بالأمن المادي بالنسبة للنتائج المباشرة يشكل أقوى ارتباط، وبلغت قيمة معاملة (0.452) في حين أن أضعف العلاقات التي ربطت الكوارث الطبيعية بالنتائج المباشرة هي مع تهديد أمن القواعد، وبلغت قيمة معاملة (0.403). وفيما يختص بالنتائج غير المباشرة، فقد كانت أعلى قيمة معامل ارتباط لها مع الموثوقية (0.427) مقابل ارتباطها مع الخصوصية بمعامل بلغت قيمته(0.359)، وهذا مؤشر على أن حدوث كارثة طبيعية ربما يكون أقوى تأثيراً على الماديات سواء كان مباني أو أجهزه ومعدات، إذ من الممكن تعويض أو تفادي تأثيره على البرمجيات من خلال الاحتفاظ بنسخ احتياطية، لكن تدمير المباني وتلف الأجهزة يحتاج إلى إعادة بناء واعادة تجهيز لهذه المباني بأجهزة ومعدات حديثة أو إصلاح الأجهزة والمعدات التي تعرضت للتهديد ان أمكن ذلك .

أما فيما يتعلق بتهديد القراصنة والمحترفين، فإنه يرتبط ارتباطاً موجباً بالنتائج المباشرة، وقد بلغ معاملة (0.204) وهو ذو دلالة إحصائية عند(α=0.05) مقابل ارتباط موجب لتهديد القراصنة والمحترفين بالنتائج غير المباشرة بلغ معامله

(0.290)، وهذا يعني أن تهديد القراصنة والمحترفين يسبب اتجاهات إيجابية في النتائج المباشرة وغير المباشرة للتهديدات الأمنية.

وبالنظر إلى النتائج الإحصائية المبينة في الجدول ذاته، يظهر أن ارتباط تهديد القراصنة والمحترفين بأمن التطبيقات وأمن الشبكات عند مستوى دلالة (α=0.05) في حين لم تظهر النتائج أية علاقة بين تهديد القراصنة والمحترفين والأمن المادي وأمن القواعد للنتائج المباشرة ، كما لم تظهر النتائج أن هنالك أية علاقة بين تهديد القراصنة والمحترفين والخصوصية للنتائج غير المباشرة، وهذا مؤشر على أن المحترفين والقراصنة عندما يهاجمون يكون هدفهم، على الأغلب، ليس الأجهزة (أي الماديات) بل البرامج والشبكات، ويكون تأثير تهديدهم على مصداقية وموثوقية المعلومات، إذ يعني إجراء تعديل أو تغيير لمحتوى البرامج فقداً للموثوقية والمصداقية، كما أن سرقة البرامج والمعلومات وعدم توافرها في وقت الحاجة لها بسب قيام القراصنة بالاعتداء عليها يفقدها تكاملها .

ويتبين من الجدول رقم(16) أن تهديد البرمجيات الخبيثة يرتبط ارتباطاً موجباً بالنتائج المباشرة، وقد بلغ معامل الارتباط (0.377) ، مقابل ارتباط موجب لتهديد البرمجيات الخبيثة بالنتائج غير المباشرة بلغ معامله (0.460)، وهذا يعني أن تهديد البرمجيات الخبيثة يسبب اتجاهات إيجابية في نتائج التهديدات الأمنية المباشرة وغير المباشرة.

وبالنظر إلى النتائج الإحصائية المبينة في الجدول ذاته، يظهر أن ارتباط تهديد البرمجيات الخبيثة بأمن التطبيقات للتهديدات المباشرة يشكل أقوى ارتباط وبلغت قيمة معاملة (0.432) في حين أن أضعف العلاقات التي ربطت بين تهديد البرمجيات الخبيثة بالنتائج المباشرة هي مع تهديد آمن الشبكات وبلغت قيمة معاملة (0.271). وفيما يختص بالنتائج غير المباشرة؛ فقد كانت أعلى قيمة معامل ارتباط لها مع التكاملية(0.502) مقابل ارتباطها مع الخصوصية بمعامل بلغت قيمته (0.359)، وهذا مؤشر على أن البرمجيات الخبيثة ، وكما هو معروف، تستغل لتدمير النظام أو البرمجيات أو الملفات. ويعمل تعرض البرمجيات إلى تهديد برمجيات خبيثة ، على الأغلب، على شطبها، وعدم وجودها عندما تحتاج إليها،

وهذا هو نقطة الارتكاز التي يستند إليها تكامل المعلومات، إذ فقدت المعلومات تكاملها، ويرجع السبب في قلة تأثير البرمجيات الخبيثة على أمن الشبكات إلى كون هذه الشبكات محصنة بشكل جيد ضد الفيروسات من خلال أجهزه حديثة ومتطورة منصوبة باستمرار على الشبكات والأجهزة الرئيسية لتواكب التطور السريع في ظهور أنواع جديدة من البرمجيات الخبيثة.

الإجابة عن سؤال الدراسة السادس الذي ينص على :

"ما هي الأهمية النسبية للبنية التحتية (التنظيمية، والتقنية، والقانونية) لأمنية المعلومات الإلكترونية "؟

ومن أجل الإجابة عن هذا السؤال تم استخراج النسب المئوية للأبعاد (التنظيمية، والتقنية، والقانونية)، بهدف التعرف على الأهمية النسبية لهذه الأبعاد وكانت النتائج على النحو التالي:

الجدول رقم (17) النسب المئوية للأبعاد (التنظيمية، والتقنية، والقانونية)

الرقم	الفقـــــرة	النسبة المئوية	
		نعم	لا
1-	هنالك قسم خاص مسؤول عن أمن المعلومات وحمايتها في المنظمة.	%70	%30
2-	هنالك أسس لتصنيف أمنية المعلومات ودرجة سريتها .	%70.9	%29.1
3-	هنالك معايير وأسس تستخدم باعتبارها ضوابط أمنية للأفراد .	%76.4	%23.6
4-	هنالك رقابة مستمرة من الإدارة العليا على الإجراءات الأمنية .	%60	%40
5-	يوجد في المنظمة وظيفة بمسمى ضابط أمن معلومات .	%14.5	%85.5
6-	توجد إجراءات تقنية في المنظمة للمحافظة على المحطات الطرفية وسلامتها.	%82.7	%17.3
7-	يتم عمل صيانة دورية لمراكز الحاسوب وتقنياته في المنظمة .	%88.2	%11.8
8-	يتم عمل صيانة دورية لأنظمة ووسائل الأمان في المنظمة .	%83.6	%16.4
9-	هنالك سجل يضبط تحركات عمال الصيانة الداخليين .	%73.6	%26.4
10-	يوجد قسم داخل المنظمة يهتم بالشؤون القانونية المتعلقة بالحاسوب.	%54.5	%45.5
11-	توجد عقوبات بحق من يعتدي على أمنية المعلومات .	%71.8	%28.2
12-	تتخذ المنظمة إجراءات صارمة بحق من يكشف أسرار العمل المتعلقة بالمهنة	%80	%20
13-	تتخذ المنظمة إجراءات صارمة بحق من يكشف أسرار العمل المتعلقة بالمراجعين ومعاملاتهم .	%79.1	%20.9
14-	تنظم عملية أمن وحماية المعلومات بوساطة السلطة التشريعية .	%60.9	%39.1

يبين الجدول رقم (17) النسبة المئوية المتعلقة بالإجابة بنعم على فقرات البعد التنظيمي التي كانت بشكل عام، وهي مرتفعة عدا النسبة المتعلقة بالفقرة رقم (5) فقد كانت منخفضة، إذ بلغت (14.5%) وتعكس تلك النسب مستوى إدراك ووعي المؤسسات المبحوثة لأهمية البنية التنظيمية التحتية لأمنية المعلومات .

أما النسب المئوية المتعلقة بالإجابة بنعم على فقرات البعد التقني من (6-9) فكانت مرتفعة مما يؤشر إلى الاهتمام الواضح من المؤسسات المبحوثة للإجراءات والأعمال المرتبطة بصيانة الأجهزة والأنظمة الإلكترونية بوصفها إجراءً مهماً وسابقاً لتهيئة هذه الوزارات للجاهزيه لتطبيق الحكومة الإلكترونية .

ما النسب المئوية المتعلقة بالإجابة بنعم على فقرات البعد القانوني من(10-14) فتوضح تباناً في قيمها تتروح بين متوسط ومرتفع، إذ حصلت الفقرات (11، 12، 13) على نسب مرتفعة بينما حصلت الفقرتان(10 ،14) على نسب مئوية متوسطة، والسبب في هذا التباين يعود إلى أن البعد القانوني الذي يرتبط بعمل الحكومي الإلكتروني ما يزال في مراحل النمو والتطور .

اختبار فرضيات الدراسة

لأجل معرفة تأثير التهديدات الداخلية لأمن المعلومات في النتائج المباشرة للتهديدات، تم إجراء تحليل الانحدار المتعدد للتأكد من صلاحية النموذج في اختبار الفرضية الأولى.

الفرضية الأولى:

لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الداخلية لأمن المعلومات ببعديها (التهديدات التقنية، والتهديدات البشرية) في النتائج المباشرة للتهديدات.

وقد تم استخدام أسلوب الانحدار المتعدد لاختبار الفرضية الأولى وكانت النتائج كما يلي:

الجدول رقم (18)

نتائج تحليل تباين الانحدار (Analysis of Variance) للتأكد من صلاحية النموذج لاختبار الفرضية الأولى.

المصدر	درجات الحرية	مجموع المربعات	متوسط المربعات	قيمة F المحسوبة	مستوى دلالة F
الانحدار	2	25.011	12.506	21.927	0.000
الخطأ	107	61.027	0.570		

* ذات دلالة إحصائية على مستوى دلالة (α =0.0001)

معامل التحديد (R^2) = 0.291

قيمة R = 0.539

قيمة (F) الجدولية عند مستوى دلالة (α =0.01) ودرجات حرية (2، 107) = (4.79)

يتبين من معطيات الجدول رقم(18)، ثبات صلاحية النموذج لاختبار الفرضية الأولى استناداً إلى ارتفاع قيمة (F) المحسوبة والبالغة(21.927)، عن قيمتها الجدولية على مستوى دلالة (α =0.01) ودرجات حرية (2، 107) = والبالغة (4.79) ، ويتضح من الجدول نفسه أن المتغير المستقل (التهديدات الداخلية) في ذلك النموذج يفسر ما مقداره (29.1%) من التباين في المتغير التابع وهي قوة تفسير متوسطة نسبياً، مما يدل على وجود اثر للمتغير المستقل في المتغير التابع وأن النموذج ذو صلاحية لاختبار الفرضية الأولى.

الجدول رقم (19)

نتائج تحليل الانحدار المتعدد لاختبار أثر التهديدات الداخلية(التهديدات التقنية، التهديدات البشرية) لأمن المعلومات في النتائج المباشرة للتهديدات .

التهديدات الداخلية	B	الخطأ المعياري	Beta	قيمة t المحسوبة	مستوى دلالة t
التهديدات التقنية	0.575	0.131	0.466	*4.389	0.000
التهديدات البشرية	0.173	0.177	0.104	0.980	0.329

*ذات دلالة إحصائية على مستوى(α=0.01).

*قيمة (t)الجدولية عند مستوى دلالة(α=0.01) ودرجات حرية (107) =2.358.

تشير المعطيات الإحصائية في الجدول رقم(19)، بالاستناد إلى قيمة(t) المحسوبة(4.389) عند مستوى دلالة(α=0.01) ودرجات حرية(107) التي كانت أكبر من قيمتها الجدولية(2.358)، أن التهديدات التقنية كانت ذات دلالة إحصائية

مهمة، وقد أسهمت في تفسير قوة التأثير في النتائج المباشرة للتهديدات ، ويعزز ذلك قيمة معامل(Beta)، البالغة(0.466)، فيما لم تظهر النتائج أي أهمية معنوية للتهديدات البشرية، إذ بلغت قيمة(t) (0.98) وقيمة معامل(Beta) (0.104).

الجدول رقم (20)

نتائج تحليل الانحدار المتعدد التدريجي (Stepwise Multiple Regression analysis) للتنبؤ (بالنتائج المباشرة للتهديدات الأمنية) من خلال أبعاد المتغير المستقل (التهديدات الداخلية).

ترتيب دخول المتغيرات في معادلة التنبؤ	معامل التحديد (R^2)	قيمة F المحسوبة	مستوى دلالة F
تهديدات تقنية	0.284	42.909	0.000

* لم تدخل (التهديدات البشرية) في معادلة الانحدار
* ذات دلالة إحصائية على مستوى دلالة (α =0.0001)
* قيمة (F) الجدولية عند مستوى دلالة (α =0.01) ودرجات حرية (108.1) = (6.85)

وعند إجراء تحليل الانحدار المتعدد التدريجي لمعرفة ترتيب دخـــول عناصـــر المتغيرات المستقلة في معادلة الانحدار يتضح من الجدول رقم(20) أن (التهديـــدات التقنية) قد دخلت فقط ، ويفسر ذلك ما مقداره(28.4%) من قيمة التغير في المتغير التابع، كما أن قيمة(F) المحسوبة قد بلغت(42.909) وهي أكبر من قيمتها الجدولية، ويعزز ذلك قيمة معامل الانحدار Beta ، و(T) التي بلغت (2.083 ، 0.533) على التوالي .

ومما سبق يقتضي ما يلي:

1. رفض الفرضية الصفرية التي تنص على أنه لا يوجد أثر ذو دلالة إحصائية للتهديدات التقنية لأمن المعلومات في النتائج المباشرة للتهديدات، وقبول الفرضية البديلة التي تنص على وجود أثر مهم ذو دلالة إحصائية للتهديدات التقنية لأمن المعلومات على النتائج المباشرة للتهديدات.
2. . قبول الفرضية الصفرية التي تنص على أنه لا يوجد اثر ذو دلالة إحصائية للتهديدات البشرية لأمن المعلومات في النتائج المباشرة للتهديدات، وذلك استنادا إلى قيمة (t) المحسوبة لهذا المتغير.

الفرضية الثانية:

لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الداخلية لأمن المعلومات ببعديها(التهديدات التقنية والتهديدات البشرية) في النتائج غير المباشرة للتهديدات.

لأجل معرفة تأثير التهديدات الداخلية لأمن المعلومات في النتائج غير المباشرة للتهديدات ، تم إجراء تحليل الانحدار المتعدد للتأكد من صلاحية النموذج في اختبار الفرضية الثانية.

الجدول رقم (21)

نتائج تحليل تباين الانحدار للتأكد من صلاحية النموذج لاختبار الفرضية الثانية.

المصدر	درجات الحرية	مجموع المربعات	متوسط المربعات	قيمة F المحسوبة	مستوى دلالة F
الانحدار	2	33.677	16.838	36.209	0.000
الخطأ	107	49.758	0.465		

* ذات دلالة إحصائية على مستوى دلالة (α =0.0001)

معامل التحديد (R^2) = 0.404

قيمة R = 0.635

قيمة (F) الجدولية عند مستوى دلالة (α =0.01) ودرجات حرية (2، 107) =4.79

يتبين من معطيات الجدول رقم(21) ثبات صلاحية النموذج لاختبار الفرضية الثانية استناداً إلى ارتفاع قيمة (F) المحسوبة البالغة(36.209) عن قيمتها الجدولية على مستوى دلالة(α =0.01) ، ودرجات حرية(2، 107) البالغة(4.79)، ويتضح من الجدول أن المتغير المستقل (التهديدات الداخلية) في النموذج يفسر ما مقداره (40.4%) من التباين في المتغير التابع، وهي قوة تفسير مرتفعه، مما يدل على وجود أثر مهم للمتغير المستقل في المتغير التابع وهذا النموذج ذو صلاحية لاختبار الفرضية الثانية.

الجدول رقم (22)

نتائج تحليل الانحدار المتعدد لاختبار أثر التهديدات الداخلية(التهديدات التقنية، التهديدات البشرية) لأمن المعلومات في النتائج غير المباشرة للتهديدات.

التهديدات الداخلية	B	الخطأ المعياري	Beta	قيمة t المحسوبة	مستوى دلالة t
التهديدات التقنية	0.759	0.118	0.625	*6.417	0.000
التهديدات البشرية	0.0255	0.160	0.016	0.160	0.873

*ذات دلالة إحصائية على مستوى(α=0.01).

*قيمة (t)الجدولية عند مستوى دلالة(α=0.01) ودرجات حرية (107) =2.358.

تشير المعطيات الإحصائية في الجدول رقم(22)، وبالاستناد إلى قيمة(t) المحسوبة (6.417)عند مستوى دلالة (α=0.01) ودرجات حرية (107)، أن التهديدات التقنية كانت ذات دلالة إحصائية مهمة وقد أسهمت في تفسير قوة التأثير في النتائج غير المباشرة للتهديدات، ويعزز ذلك قيمة معامل(Beta)، البالغة (0.625)، فيما لم تظهر النتائج أي أهمية معنوية للتهديدات البشرية، إذ بلغت قيمة (t) (0.160) وقيمة معامل(Beta)(0.016) .

ومما سبق يقتضي ما يلي:

1. رفض الفرضية الصفرية التي تنص على أنه لا يوجد أثر ذو دلالة إحصائية للتهديدات التقنية لأمن المعلومات في النتائج غير المباشرة للتهديدات، وقبول الفرضية البديلة التي تنص على وجود أثر مهم ذي دلالة إحصائية للتهديدات التقنية لأمن المعلومات في النتائج غير المباشرة للتهديدات .

3. قبول الفرضية الصفرية التي تنص على أنه لا يوجد أثر ذو دلالة إحصـــائية للتهديدات البشرية لأمن المعلومات في النتائج غير المباشرة للتهديدات، وذلك استنادا إلى قيمة (t) المحسوبة لهذا المتغير.

الجدول رقم (23)

نتائج تحليل الانحدار المتعدد التدريجي (Stepwise Multiple Regression analysis) للتنبؤ (بالنتائج غير المباشرة للتهديدات الأمنية) من خلال أبعاد المتغير المستقل (التهديدات الداخلية).

ترتيب دخول المتغيرات في معادلة التنبؤ	معامل التحديد (R^2)	قيمة F المحسوبة	مستوى دلالة F
تهديدات تقنية	0.403	73.052	0.000

* لم تدخل (التهديدات البشرية) في معادلة الانحدار
* ذات دلالة إحصائية على مستوى دلالة (α =0.0001)
* قيمة (F) الجدولية عند مستوى دلالة (α =0.01) ودرجات حرية (108.1) = (6.85)

وعند إجراء تحليل الانحدار المتعدد التدريجي لمعرفة ترتيب دخول عناصر المتغيرات المستقلة في معادلـــة الانحـــدار يتضـــح مـــن الجـــدول رقـــم(23)

ان(التهديدات التقنية) قد دخلت فقط ، ويفسر ذلك ما مقداره(40.3%) من قيمة التغير في المتغير التابع، كما أن قيمة(F) المحسوبة قد بلغت(73.052) وهي أكبر من قيمتها الجدولية، ويعزز ذلك قيمة معامل الانحدار Beta ،و(T) التي بلغت(8.547 , 0.635) على التوالي .

الفرضية الثالثة:

لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الخارجية لأمن المعلومات بأبعادها (الكوارث الطبيعية، والقراصنة والمحترفين، والبرمجيات الخبيثة) في النتائج المباشرة للتهديدات .

لأجل معرفة تأثير التهديدات الخارجية لأمن المعلومات في النتائج المباشرة للتهديدات ، تم إجراء تحليل الانحدار المتعدد للتأكد من صلاحية النموذج في اختبار الفرضية الثالثة.

الجدول رقم (24)

نتائج تحليل تباين الانحدار للتأكد من صلاحية النموذج لاختبار الفرضية الثالثة.

المصدر	درجات الحرية	مجموع المربعات	متوسط المربعات	قيمة F المحسوبة	مستوى دلالة F
الانحدار	3	20.733	6.911	11.218	0.000
الخطأ	106	65.305	0.616		

* ذات دلالة إحصائية على مستوى دلالة (α =0.0001)
* معامل التحديد (R^2) =0.241
* قيمة R = 0.491
* قيمة (F) الجدولية عند مستوى دلالة (α =0.01) ودرجات حرية (3، 106) =3.95

يتبين من معطيات الجدول رقم(24) ثبات صلاحية النموذج لاختبار الفرضية الثالثة استناداً إلى ارتفاع قيمة(F) المحسوبة والبالغة(11.218) عن قيمتها الجدولية على مستوى دلالة (α =0.01) ، ودرجات حرية(106.3) والبالغة(3.95)، ويتضح من الجدول المذكور ان المتغير المستقل (التهديدات الخارجية) في النموذج يفسر ما مقداره (24.1%) من التباين في المتغير التابع، وهي قوة تفسير متوسطة نسبياً، مما يدل على وجود أثر مهم للمتغير المستقل في المتغير التابع، وأن النموذج ذو صلاحية لاختبار الفرضية الثالثة .

الجدول رقم (25)

ملخص نتائج تحليل الانحدار المتعدد لاختبار أثر التهديدات الخارجية(الكوارث الطبيعية، والقراصنة والمحترفين، والبرمجيات الخبيثة) لأمن المعلومات في نتائج التهديدات المباشرة.

التهديدات الخارجية	B	الخطأ المعياري	Beta	قيمة t المحسوبة	مستوى دلالة t
كوارث طبيعية	0.412	0.112	0.364	*3.688	0.000
المحترفون والقراصنة	0.121	0.132	0.101	0.923	0.358
البرمجيات الخبيثة	0.320	0.145	0.256	**2.214	0.029

*ذات دلالة إحصائية على مستوى(α=0.01).

** ذات دلالة إحصائية على مستوى(α=0.05).

*قيمة (t)الجدولية عند مستوى دلالة(α=0.01) ودرجات حرية (106) =2.358.

تشير المعطيات الإحصائية في الجدول رقم(25)، وبالاستناد إلى قيمة(t) المحسوبة (3.688) عند مستوى دلالة(α=0.01) ودرجات حرية(106)، أن الكوارث الطبيعية كانت ذات دلالة إحصائية مهمة وقد أسهمت في تفسير قوة التأثير في النتائج المباشرة للتهديدات ، ويعزز ذلك قيمة معاملات(Beta)، البالغة (0.364)

كما يتضح من الجدول أن البرمجيات الخبيثة كانت ذات دلالة إحصائية مهمة عند مستوى دلالة(α=0.05) ودرجات حرية(106)، حيث بلغت قيمة(t) لهذا المتغير(2.214) ، ويعزز ذلك قيمة معامل (Beta)، البالغة قيمتها (0.320)، فيما لم تظهر النتائج أي أهمية معنوية للمحترفين والقراصنة، اذ بلغت قيمة(t) (0.923) وقيمة معامل(Beta)(0.121) .

ومما سبق يقتضي ما يلي:

1. رفض الفرضية الصفرية التي تنص على أنه لا يوجد أثر ذو دلالة إحصائية للكوارث الطبيعية لأمن المعلومات في النتائج المباشرة للتهديدات، وقبول الفرضية البديلة التي تنص على وجود أثر مهم ذي دلالة إحصائية للكوارث الطبيعية لأمن المعلومات في النتائج المباشرة للتهديدات .

2. رفض الفرضية الصفرية التي تنص على أنه لا يوجد أثر ذو دلالة إحصائية للبرمجيات الخبيثة لأمن المعلومات في النتائج المباشرة للتهديدات، وقبول الفرضية

البديلة التي تنص على وجود أثر مهم ذي دلالة إحصائية للبرمجيات الخبيثة لأمن المعلومات في النتائج المباشرة للتهديدات.

3-.قبول الفرضية الصفرية التي تنص على أنه لا يوجد أثر ذو دلالة إحصائية للمحترفين والقراصنة لأمن المعلومات في النتائج المباشرة للتهديدات، وذلك استنادا إلى قيمة (t) المحسوبة لهذا المتغير، لأن الحكومة الإلكترونية في مراحلها الأولى والاتصال فيها أحادي الجانب .

الجدول رقم (26)

نتائج تحليل الانحدار المتعدد التدريجي (Stepwise Multiple Regression analysis) للتنبؤ (بالنتائج غير المباشرة للتهديدات الأمنية) من خلال أبعاد المتغير المستقل (التهديدات الخارجية).

ترتيب دخول المتغيرات في معادلة التنبؤ	معامل التحديد (R^2)	قيمة F المحسوبة	مستوى دلالة F
كوارث طبيعية	0.205	27.888	0.000
برمجيات خبيثة	0.235	16.424	0.000

* لم يدخل (المحترفون والقراصنة) في معادلة الانحدار
* ذات دلالة إحصائية على مستوى دلالة (α =0.0001)
* قيمة (F) الجدولية عند مستوى دلالة (α =0.01) ودرجات حرية (108.1) = 6.85
* قيمة (F) الجدولية عند مستوى دلالة (α =0.01) ودرجات حرية (107.2) = 4.79

وعند إجراء تحليل الانحدار المتعدد التدريجي لمعرفة ترتيب دخول عناصر المتغيرات المستقلة في معادلة الانحدار، يتضح من الجدول رقم(26) أن (الكوارث الطبيعية والبرمجيات الخبيثة) قد دخلت فقط ، ويفسر ذلك ما مقداره (23.5، 20.5) على التوالي، من قيمة التغير في المتغير التابع كما أن قيمة(F) المحسوبة قد بلغت(27.888، 16.424) على التوالي ، وهي أكبر من قيمتها الجدولية ، ويعزز ذلك قيمة معامل الانحدار Beta ، و(T) التي بلغت على التوالي (0.453 ،5.281)، (0.199 ، 2.036).

الفرضية الرابعة :

لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الخارجية لأمن المعلومات بأبعادها (الكوارث الطبيعية، والقراصنة والمحترفين، والبرمجيات الخبيثة) في النتائج غير المباشرة للتهديدات .

لأجل معرفة تأثير التهديدات الخارجية لأمن المعلومات في نتائج التهديدات غير المباشرة، تم إجراء تحليل الانحدار المتعدد للتأكد من صلاحية النموذج في اختبار الفرضية الرابعة.

الجدول رقم (27)

نتائج تحليل تباين الانحدار للتأكد من صلاحية النموذج لاختبار الفرضية الرابعة

المصدر	درجات الحرية	مجموع المربعات	متوسط المربعات	قيمة F المحسوبة	مستوى دلالة F
الانحدار	3	22.350	7.450	12.928	0.000
الخطأ	106	61.084	0.576		

* ذات دلالة إحصائية على مستوى دلالة (α =0.0001)

معامل التحديد (R^2) = 0.268

قيمة R = 0.518

قيمة (F) الجدولية عند مستوى دلالة (α =0.01) ودرجات حرية (3، 106) = 3.95

يتبين من معطيات الجدول رقم(27) ثبات صلاحية النموذج لاختبار الفرضية الرابعة استناداً إلى ارتفاع قيمة(F) المحسوبة والبالغة(12.928) عن قيمتها الجدولية على مستوى دلالة(α =0.01)، ودرجات حرية(106.3) والبالغة(3.95)، ويتضح من الجدول المذكور أن المتغير المستقل(التهديدات الخارجية) في النموذج يفسر ما مقداره(26.8%) من التباين في المتغير التابع، وهي قوة تفسير متوسطة نسبياً ، مما يدل على وجود أثر مهم للمتغير المستقل في المتغير التابع، وأن النموذج ذو صلاحية لاختبار الفرضية الرابعة .

الجدول رقم (28)

نتائج تحليل الانحدار المتعدد لاختبار أثر التهديدات الخارجية(الكوارث الطبيعية، والمحترفين، والبرمجيات الخبيثة) لأمن المعلومات في النتائج غير المباشرة للتهديدات.

التهديدات الخارجية	B	الخطأ المعياري	Beta	قيمة t المحسوبة	مستوى دلالة t
كوارث طبيعية	0.307	0.108	0.267	*2.854	0.005
المحترفون والقراصنة	0.0392	0.127	0.033	0.308	0.759
البرمجيات الخبيثة	0.421	0.140	0.342	*3.008	0.003

*ذات دلالة إحصائية على مستوى(α=0.01).

*قيمة (t)الجدولية عند مستوى دلالة(α=0.01) ودرجات حرية (106) =2.358.

تشير المعطيات الإحصائية في الجدول رقم(28)، وبالنظر إلى قيم(t) المحسوبة (2.845 ، 3.008) على التوالي عند مستوى دلالة (α=0.01) ودرجات حرية (106)، ان الكوارث الطبيعية والبرمجيات الخبيثة كانتا ذات دلالة إحصائية مهمة وقد أسهمتا في تفسير قوة التأثير في النتائج غير المباشرة للتهديدات، ويعزز ذلك قيمة معاملات(Beta)، البالغة (0.307، 0.421) على التوالي.

فيما لم تظهر النتائج أي أهمية معنوية للمحترفين والقراصنة، إذ بلغت قيمة(t) (0.308) وقيمة معامل(Beta)(0.033) .

ومما سبق يقتضي ما يلي:

1. رفض الفرضية الصفرية التي تنص على أنه لا يوجد أثر ذو دلالة إحصائية للكوارث الطبيعية لأمن المعلومات في النتائج غير المباشرة للتهديدات، وقبول الفرضية البديلة التي تنص على وجود أثر مهم ذي دلالة إحصائية للكوارث الطبيعية لأمن المعلومات في النتائج غير المباشرة للتهديدات .
2. رفض الفرضية الصفرية التي تنص على انه لا يوجد أثر ذو دلالة إحصائية للبرمجيات الخبيثة لأمن المعلومات في النتائج غير المباشرة للتهديدات ، وقبول الفرضية البديلة التي تنص على وجود أثر مهم ذي دلالة إحصائية للبرمجيات الخبيثة لأمن المعلومات في النتائج غير المباشرة للتهديدات.

3. قبول الفرضية الصفرية التي تنص على أنه لا يوجد أثر ذو دلالة إحصائية المحترفين والقراصنة لأمن المعلومات على النتائج غير المباشرة للتهديدات وذلك استنادا إلى قيمة(t) المحسوبة لهذا المتغير.

الجدول رقم (29)

نتائج تحليل الانحدار المتعدد التدريجي (Stepwise Multiple Regression analysis) للتنبؤ (بالنتائج غير المباشرة للتهديدات الأمنية) من خلال أبعاد المتغير المستقل (التهديدات الخارجية).

ترتيب دخول المتغيرات في معادلة التنبؤ	معامل التحديد (R^2)	قيمة F المحسوبة	مستوى دلالة F
كوارث طبيعية	0.189	25.195	0.000
برمجيات خبيثة	0.267	19.510	0.000

* لم يدخل (المحترفون والقراصنة) في معادلة الانحدار
* ذات دلالة إحصائية على مستوى دلالة (α =0.0001)
* قيمة (F) الجدولية عند مستوى دلالة (α =0.01) ودرجات حرية (108.1) = 6.85
* قيمة (F) الجدولية عند مستوى دلالة (α =0.01) ودرجات حرية (107.2) = 4.79

وعند إجراء تحليل الانحدار المتعدد التدريجي لمعرفة ترتيب دخول عناصر المتغيرات المستقلة في معادلة الانحدار، يتضح من الجدول رقم(29) أن(الكوارث الطبيعية والبرمجيات الخبيثة) قد دخلت فقط، ويفسر ذلك ما مقداره (18.9،26.7) على التوالي من قيمة التغير في المتغير التابع كما أن قيمة(F) المحسوبة قد بلغت (25.195، 19.510) على التوالي، وهي أكبر من قيمتها الجدولية ، ويعزز ذلك قيمة معامل الانحدار Beta ، و(T) التي بلغت على التوالي (0.435، 5.019) ، (0.323 ، 3.376) .

الفرضية الخامسة: لا تختلف تصورات المبحوثين لنتائج التهديدات الأمنية باختلاف المتغيرات الديموغرافية مثل:(الجنس، والعمر، والمؤهل العلمي، وسنوات الخبرة، والمسمى الوظيفي).

الجدول رقم (30)

نتائج تحليل التباين الأحادي (ANOVA) لدرجة تأثير المتغيرات الديموغرافية في تصورات المبحوثين لنتائج التهديدات الأمنية.

اسم المتغير	فئة المتغير	درجات الحرية	المتوسط الحسابي	قيمة (F) المحسوبة	مستوى دلالة (F)
الجنس	ذكر	(1، 108)	3.5449	*6.346	0.013
	أنثى		3.1277		
العمر	29 سنة فأقل	(3، 106)	3.4692	*4.478	0.019
	30-39 سنة		3.6027		
	40-49 سنة		2.9830		
	50 سنة فأكثر		2.7469		
المؤهل العلمي	الثانوية العامة فما دون	(3، 106)	2.6707	*8.231	0.000
	الدبلوم المتوسط		2.9672		
	البكالوريوس		3.6252		
	الدراسات العليا		2.5759		
الخبرة	5 سنوات فأقل	(3، 106)	3.5061	1.551	0.206
	6-10 سنوات		3.4933		
	11-15 سنة		3.2435		
	16 سنة فأكثر		3.0107		
المسمى الوظيفي	الإداريون	(3، 106)	3.3677	*3.643	0.015
	المبرمجون		3.6380		
	الفنيون		3.1773		
	مدخلو البيانات		2.9855		

* ذات دلالة إحصائية على مستوى دلالة (α= 0.01)

قيمة (F) الجدولية على مستوى دلالة (α= 0.01) ودرجات حرية (3، 106) = 3.95

قيمة (F) الجدولية على مستوى دلالة (α= 0.05) ودرجات حرية (3، 106) =2.68

قيمة (F) الجدولية على مستوى دلالة (α= 0.05) ودرجات حرية (1، 108) =3.92

تشير المعطيات الإحصائية في الجدول رقم (30) إلى وجود فروقات ذات دلالة إحصائية بين تصورات المبحوثين إزاء نتائج التهديدات الأمنية تعـزى لمتغيـرات

مثل: (الجنس، والعمر، والمؤهل العلمي، والمسمى الوظيفي)، مما يقتضي رفض الفرضية العدمية جزئياً التي تنص على أنه لا توجد فروقات ذات دلالة إحصائية بين تصورات المبحوثين إزاء نتائج التهديدات الأمنية تعزى للمتغيرات الديموغرافية مثل: (الجنس، والعمر، والمؤهل العلمي، والمسمى الوظيفي) باستثناء متغير (الخبرة)، وقبول الفرضية البديلة جزئياً التي تنص على أنه توجد فروقات ذات دلالة إحصائية بين تصورات المبحوثين إزاء نتائج التهديدات الأمنية تعزى لمتغيرات (الجنس، العمر، المؤهل العلمي، والمسمى الوظيفي)، بدليل ارتفاع قيم(F) المحسوبة عن قيمتها الجدولية، وقيم(F) المحسوبة للجنس(6.346)،وللعمر(4.478) وللمؤهل العلمي(8.231)، وللمسمى الوظيفي(3.643) وجميع قيم(F) المحسوبة تلك ذات دلالة إحصائية على مستوى دلالة(α= 0.01) و(α= 0.05) بينما بلغت قيمة متغير (الخبرة) (1.551) وهي ليست ذات دلاله إحصائية .

وفيما يتعلق بنتائج اختبار شيفيه(Scheffe) للمقارنات البُعدية، يتضح ما يلي:

أ- متغير الجنس، كانت مصادر الفروق لصالح الذكور، إذ بلغ متوسط الذكور (3.5449)، أما متوسط الإناث، فقد بلغ (3.1277)، كما يشير الجدول رقم(30) ويمكن تفسير هذه النتيجة بأن الذكور أكثر تصوراً وإدراكاً للنتائج المباشرة وغير المباشرة لتهديدات أمنية المعلومات .

ب- متغير العمر، كانت مصادر الفروق بين الفئات العمرية(30-39 سنة) والفئة الثالثة(40-49سنة) لصالح الفئة العمرية (30-39 سنة) إذ بلغ متوسط هذه الفئة (3.6027)، أما متوسط الفئة الثالثة (40-49سنة) فقد بلغ(2.9830). ويمكن تفسير هذه النتيجة بأن الفئة العمرية من (30-39) هي أكثر الفئات تصوراً للنتائج المباشرة وغير المباشرة للتهديدات الأمنية وان هذه الفئة تمتلك ،على الأغلب ، الشروط والرغبة في التأثير في مجريات الأمور .

جـ- متغير المؤهل العلمي،كانت مصادر الفروق بين المؤهلات العلمية الفئه الثالثة (البكالوريوس) والفئة الثانية (الدبلوم المتوسط) لصالح الفئة الثالثة البكالوريوس اذ بلغ متوسط هذه الفئة (3.6252)، أما متوسط الفئة الثانية(الدبلوم المتوسط) فقد بلغ(2.9672) ، وكانت مصادر الفروق بين المؤهلات العلمية(البكالوريوس) والفئة

الرابعة (الدراسات العليا) لصالح الفئة الثالثة البكالوريوس إذ بلغ متوسط هذه الفئة (3.6252)، أما متوسط الفئة الرابعة(الدراسات العليا) فقد بلغ(2.5759) وتفسر هذه النتيجة بأن فئة البكالوريوس أكثر فئات المبحوثين تصوراً للنتائج المباشرة وغير المباشرة للتهديدات لاسيما وأنها تمتلك مؤهلاً يعتبر كافياً لمعرفة بيئة التهديد ونتيجته المباشرة وغير المباشرة .

د-متغير المسمى الوظيفي،كانت مصادر الفروق بين فئات المسمى الوظيفي(المبرمجين)والفئة الرابعة(مدخلي البيانات) لصالح الفئة الثانية (المبرمجين) إذ بلغ متوسط هذه الفئة (3.6280)، أما متوسط الفئة الرابعة(مدخلي البيانات) فقد بلغ(2.9855)،وتشير هذه النتيجة إلى تفسير مفاده أن المسمى الوظيفي(المبرمجين) هم أكثر الفئات الوظيفية سلطة ومعرفة فنية وتصوراً للنتائج المباشرة وغير المباشرة للتهديدات الأمنية،(فالمبرمج)هو الأكثر وصولاً وتأثيراً بالمواد البرامج بحكم التخصص الدقيق والإلمام الواسع ببرمجيات الأعمال الإلكترونية .

الجدول رقم(31)

نتائج اختبار شيفيه للمقارنات البُعدية للمتغيرات الديموغرافية في نتائج التهديدات الأمنية

متغير العمر

فئات العمر	29 سنة فأقل 3.4692	30-39 سنة 3.6027	40-49 سنة 2.9830	50 سنة فأكثر 2.7469
29 سنة فأقل	-	-	-	-
30-39 سنة	-	-	-	-
40-49 سنة	-	*0.6197	-	-
50 سنة فأكثر	-	-	-	-

* ذات دلالة إحصائية على مستوى (α = 0.05)

المؤهل العلمي

فئات المؤهل العلمي	الثانوية العامة فما دون 2.6707	الدبلوم المتوسط 2.9672	البكالوريوس 3.6252	الدراسات العليا 2.5759
الثانوية العامة فما دون	-	-	-	-
الدبلوم المتوسط	-	-	*0.6580	-
البكالوريوس	-	-	-	-
الدراسات العليا	-	-	*1.049	-

* ذات دلالة إحصائية على مستوى (α = 0.05)

المسمى الوظيفي.

فئات المسمى الوظيفي	إداريين 3.3677	مبرمجين 3.6380	فنيين 3.1773	مدخلين بيانات 2.9855
الإداريون	–	–	–	–
المبرمجون	–	–	–	–
الفنيون	–	–	–	–
مدخلو البيانات	–	*0.6525	–	–

* ذات دلالة إحصائية على مستوى (α = 0.05)

الفصل الخامس

مناقشة النتائج والتوصيات

مناقشة النتائج

تمت الإجابة على أسئلة الدراسة وفرضياتها باستخدام الأساليب المناسبة ويبين الجدول رقم (32) ملخص نتائج اختبار فرضيات الدراسة

الجدول (32)ملخص نتائج اختبار فرضيات الدراسة

رقم الفرضية	الفرضية	النتيجة
الأولى	لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الداخلية لأمن المعلومات ببعديها (التهديدات التقنية والتهديدات البشرية) في النتائج المباشرة للتهديدات.	
	أ- لا يوجد أثر ذو دلالة إحصائية للتهديدات التقنية في النتائج المباشرة للتهديدات	رفض
	ب-لا يوجد أثر ذو دلالة إحصائية للتهديدات البشرية في النتائج المباشرة للتهديدات.	قبول
الثانية	لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الداخلية لأمن المعلومات ببعديها (التهديدات التقنية والتهديدات البشرية) في النتائج غير المباشرة للتهديدات .	
	أ- لا يوجد أثر ذو دلالة إحصائية للتهديدات التقنية في النتائج غير المباشرة للتهديدات.	رفض
	ب-لا يوجد أثر ذو دلالة إحصائية للتهديدات البشرية في النتائج غير المباشرة للتهديدات.	قبول
الثالثة	لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الخارجية لأمن المعلومات بأبعادها (الكوارث الطبيعية ، والقراصنة والمحترفين ، والبرمجيات الخبيثة) على النتائج المباشرة للتهديدات.	
	أ- لا يوجد أثر ذو دلالة إحصائية للتهديدات (الكوارث الطبيعية) في النتائج المباشرة للتهديدات .	رفض
	ب- لا يوجد أثر ذو دلالة إحصائية لتهديدات (القراصنة والمحترفين) في النتائج المباشرة للتهديدات .	قبول
	ج- لا يوجد أثر ذو دلالة إحصائية لتهديدات (البرمجيات الخبيثة) على النتائج المباشرة للتهديدات .	رفض
الرابعة	لا يوجد أثر هام ذو دلالة إحصائية للتهديدات الخارجية لامن المعلومات بأبعادها (الكوارث الطبيعية ، و القراصنة والمحترفين ،و البرمجيات الخبيثة) في النتائج غير المباشرة للتهديدات .	
	أ- لا يوجد أثر ذو دلالة إحصائية لتهديدات (الكوارث الطبيعية) في النتائج غير المباشرة للتهديدات .	رفض
	ب- لا يوجد أثر ذو دلالة إحصائية لتهديدات (القراصنة والمحترفين) في النتائج غير المباشرة للتهديدات .	قبول
	ج- لا يوجد أثر ذو دلالة إحصائية لتهديدات (البرمجيات الخبيثة) في النتائج غير المباشرة للتهديدات	رفض
الخامسة	لا تختلف تصورات المبحوثين لنتائج التهديدات الأمنية باختلاف المتغيرات الديموغرافية "الجنس،و العمر ،والمؤهل العلمي،والخبرة ،والمسمى الوظيفي" .	رفض

فيما يلي أبرز النتائج التي توصلت إليها الدراسة :-

1- إن مستوى إجابات المبحوثين عن التهديدات التقنية كمهدد داخلي مرتفع ، وبلغ متوسطه الحسابي (3.8036) وفق الجدول رقم (4) اذ توصلت الدراسة إلى أن المبحوثين يستشعرون بوجود تأثيرات للتهديدات الداخلية الناتجة عن تهديد تقني على أمنية المعلومات ، ويمكن تفسير ذلك إلى حداثة عهد الاتجاه الإلكتروني في العمل الحكومي ، وأن اغلب التهديدات في المراحل الأولى من التطبيق ستكون مرتبطة بالتقنيات ، لكن بعد التشغيل وبدء العمل الإلكتروني الكامل ستظهر تهديدات أخرى جديدة ، فالتجهيزات الحالية في الوزارات المبحوثة هي استعدادات تقنية بحتة للبنية التحتية من أجل تجهيز هذه الوزارات للتحول نحو العمل الإلكتروني .

2-إن مستوى إجابات المبحوثين عن التهديدات البشرية كمهدد داخلي متوسط وبلغ متوسطة الحسابي (3.4989) وفق الجدول رقم (5) ويعود ذلك إلى أن الاتصالات الإلكترونية أحادية الجانب ، فالعنصر البشري لم يدخل بعد بشكل مباشر في اتصالات الحكومة الإلكترونية حتى يشكل تهديداً على أمنيتها ، كما يعود ذلك إلى أن العنصر البشري الذي يتعامل مع العمل الإلكتروني هو من المواطنين والعاملين الذين ، كما أشارت النتائج ، إلى أنهم أصحاب خبرة ووعي مما يساعد على عدم تشكيلهم كمهدد بل أن الموظف الواعي والأمين يشكل خط دفاع وليس هجوماً عن المؤسسة التي يعمل بها .

3-إن مستوى إجابات المبحوثين عن الكوارث الطبيعية كمهدد خارجي كان مرتفع وبلغ متوسطه الحسابي (3.5436) وفق الجدول رقم (6) يعود ذلك إلى إتصاف نظم المعلومات وتقنياتها بالحساسية العالية فأي تهديد طبيعي بهيئة كارثة (انقطاع تيار كهربائي ، فيضانات ، زلزال ، حرب) لابد أن يكون تأثيره كبير على الأجزاء المادية والبرمجيات في نظم المعلومات فيسبب الخطورة العالية والدمار الكبير الذي تلحقه الكارثة الطبيعية بالأجهزة والماديات كانت إجابات أفراد العينة ذات أهمية نسبية ومتوسط حسابي (مرتفع) .

4-إن مستوى إجابات المبحوثين عن المحترفين والقراصنة كمهدد خارجي كان مرتفعاً وبلغ متوسطة الحسابي (3.7242) وفق الجدول رقم (7) وهذا يشير إلى أن أمن المعلومات معرض للتهديد من قبل عنصر خارجي يتمثل في القراصنة والمحترفين الذين يحتاج ضبطهم ورصد تحركاتهم إلى تكاليف كبيرة ، وكلك إلى استخدام وسائل حديثة مما يستدعي من الوزارات المبحوثة التيقظ والحذر من خطورة هذا المصدر قبل بدء العمل الإلكتروني وتعرضه لهذا التهديد .

5-إن مستوى إجابات المبحوثين عن البرمجيات الخبيثة كمهدد خارجي لأمنية المعلومات كان مرتفعاً ، وبلغ متوسطة الحسابي (3.7985) وفق الجدول رقم (8) ويمكن تفسير ذلك بأن الوزارات المبحوثة معترفة بأن البرمجيات الخبيثة صاحبة تهديد وأثر في أمنية المعلومات ، وذلك من خلال حرص تلك الوزارات على استخدام أجهزة مضادة للفيروسات لكن البرمجيات الخبيثة يصعب إيقاف تهديدها بسبب مايظهر فيها من أنواع جديدة بشكل مستمر وبصفه لانهائية ، فيتم استخدام أجهزه مضادة للبرمجيات التي لم يتم بعد اكتشاف أدوات وأجهزه مضادة لها .

6-إن مستوى إجابات المبحوثين عن تهديد الأمن المادي كنتيجة مباشرة للتهديدات كان متوسطاً وبلغ متوسطة الحسابي (3.2400) وفق الجدول رقم (9) إذ إن المبحوثين لديهم قناعه بأن حداثة الأجهزة والمعدات وحدها لا تكفي لمنع حدوث تهديد لأمنية المعلومات ، ويمكن تفسير ذلك بضرورة دعم (الماديات الحديثة) الأجهزة والمعدات الحديثة بوسائل حماية مساندة فنية وغير فنية ، حتى تتكامل أطراف الحماية.

7-إن مستوى إجابات المبحوثين عن تهديد أمن التطبيقات كنتيجة مباشرة للتهديدات كان متوسطاً ، وبلغ متوسطة الحسابي (3.3121) وفق الجدول رقم (10) ويمكن تفسير ذلك بأن تغطية العمل الإلكتروني ماتزال جزئية ، ولم تكتمل بعد التطبيقات الكاملة للعمل الإلكتروني ، فالوزارات المبحوثة تسير في خطوة انتقالية من المرحلة الثانية إلى المرحلة الثالثة للحكومة الإلكترونية ، والبرمجيات والتطبيقات مايزال استخدامها في العمل الإلكتروني في مراحل محدودة ، وعليه ، فأن تعرضها لتهديد فعلي يُعد مبكراً في الوقت الحالي.

8-إن مستوى إجابات المبحوثين عن تهديد أمن قواعد البيانات كنتيجة مباشرة للتهديدات، كان متوسطاً ، وبلغ متوسطة الحسابي (3.3333) وفق الجدول رقم (11) وهذا يشير إلى أن الخطر الحقيقي الذي يعترض أمن قواعد البيانات هو عندما يتم الاستخدام الفعلي من المواطنين والموظفين ، لأن عدم تحديد الفئات المختصة والمخولة باستخدام قواعد البيانات هو أكثر ما يهدد أمنها .

9- إن مستوى إجابات المبحوثين عن تهديد أمن الشبكات كنتيجة مباشرة للتهديدات كان متوسطاً ، وبلغ متوسطة الحسابي (3.3591) وفق الجدول رقم (12) وهذا يشير إلى أن نوع الشبكات المستخدمة والمشكلات التي تعاني منها الأنظمة المساندة للشبكات هما الخطر الحقيقي الذي يهدد أمن الشبكات ، وهذا مؤشر على أن مصدر التهديد هو تقني أكثر منه بشري .

10-إن مستوى إجابات المبحوثين عن تهديد الموثوقية كنتيجة غير مباشرة للتهديدات كان مرتفعاً ، وبلغ متوسطه الحسابي (3.5485) وفق الجدول رقم (13) ويمكن أن يفسر ذلك بأن العمل الإلكتروني في الوازرات المبحوثة يتميز بالموثوقية والمصداقية حتى هذه المرحلة ، وهذا مؤشر على حسن اختيار الوزارات المبحوثة لموظفيها وعلى اهتمامها بتطوير مهاراتهم وخبراتهم ، لأن مايدعم الموثوقية ، بشكل أساسي ، هو حرص الموظف على سرية المعلومات التي بين يديه سواء كانت خاصة بالعمل أو المواطنين.

11-إن مستوى إجابات المبحوثين عن تهديد الخصوصية كنتيجة غير مباشرة للتهديدات كان متوسطاً ، وبلغ متوسطة الحسابي (3.3364) وفق الجدول رقم (14) ويمكن تفسير ذلك بأن شكوى المتعاملين مع الوزارات بانتهاك مبدأ الخصوصية يعد مرحله متقدمة ، فمن المبكر جداً الشكوى من انتهاك الخصوصية في هذه المرحلة قبل أن نصل إلى تطبيق كامل وفعلي للحكومة الإلكترونية .

12-إن مستوى إجابات المبحوثين عن تهديد التكاملية كنتيجة غير مباشرة للتهديدات كان مرتفعاً ، وبلغ متوسطة الحسابي (3.5182) وفق الجدول رقم (15) ويشير هذا إلى عمل جميع البرامج في الوزارات المبحوثة بشكل يؤدي إلى سلامة المعلومات ،

هذا بالإضافة إلى عدم تعرض محتوى المعلومات إلى التعديل أو التحريف ، وهـــي نتيجة تعكس واقع الحكومة الإلكترونية في المرحلة التجريبية لها .

13-وباستقراء النتائج الواردة في الجدول رقم (16) يتبين أن هناك ارتباطاً موجبـــاً بين متغيرات الدراسة المستقلة (التهديدات الداخلية والخارجية) والمتغيــر التـــابع (نتائج التهديدات المباشرة وغير المباشرة) على المستوى الكلـــي وعلـــى مســـتوى المتغيرات الفرعية ، إذ كانت علاقات الارتباط بشكل عام موجبة ، وتتروواح قوتهـــا بين متوسطة ودون المتوسط .

14- تبين إجابات المبحوثين عن الأسئلة الاستكشافية بأبعادها (التنظيمية ، والتقنية، والقانونية) في الجدول رقم (17) أن النسب المئوية للإجابة عن البعد التنظيمي كانت مرتفعة ، وكذلك عن البعد التقني ، وهذا مؤشر على الاهتمام الكبير في الـــوزارات المبحوثة بتهيئة الوزارات ، تنظيمياً وتقنياً ، للتحول نحو الحكومة الإلكترونية أمـــا البعد القانوني ، فكانت النسب المئوية متفاوتة ، وهذا يعكس الواقع القانوني المتعلق بالحكومة الإلكترونية الذي مايزال في طور النمو والتحـــديث ليواكـــب التطـــورات الحاصلة على صعيد الحكومة الإلكترونية وما تتعرض له من جرائم ذات طابع جديد وغريب .

15-توصلت الدراسة إلى وجود أثر ذي دلالة إحصائية للتهديدات الداخلية (التقنية) في النتائج المباشرة للتهديدات بقوه تفسيرية متوسطة بلغت (29.1%) وفق الجداول رقم (18) و(19) و(20)، أما عن التهديدات الداخلية البشرية ، فلم يتم التوصل إلى وجود أثر ذي دلالة إحصائية له في النتائج المباشرة ، ويمكن تفســير ذلــك بـــأن التهديدات الداخلية البشرية هي التهديدات الناتجة عن العاملين في داخـــل المنظمـــة وعدم وجود تهديد من قبلهم هو مؤشر إيجابي ينم عن امـــتلاك العـــاملين الخبـــرة والتأهيل العلمي ، كما يدل على مستوى الوعي العـــالي لـــديهم تجـــاه التهديـــدات وحرصهم على أعمالهم وعلى الأمانة التي بين أيديهم ، وأيضاً يشير ذلك إلـــى أن العمل الإلكتروني لم يكتمل بعد فهو في مرحلته الأولى ، فالمساحة المتاحة للمشاركة لدى العنصر البشري تعتبر مساحة ضيقة لم تصل بعد إلى مستوى التهديد .

16- توصلت الدراسة إلى وجود أثر ذي دلالة إحصائية للتهديدات الداخلية (التقنية) في النتائج غير المباشرة للتهديدات بقوه تفسيرية مرتفعة بلغت (40.4%) وفق الجداول رقم (21) و(22) و(23)، أما عن التهديدات الداخلية البشرية ، فلم يتم التوصل إلى وجود أثر ذي دلالة إحصائية له في النتائج غير المباشرة ، وكانت هذه النتائج متعارضة جزئياً مع نتائج دراسة (البياتي ،1996) التي وجدت أن أكثر مصدر يهدد الأمنية هو المصدر البشري الداخلي ، ووصلت نسبة تأثيره من (70-80%) .

17-توصلت الدراسة إلى وجود أثر ذي دلالة إحصائية للتهديدات الخارجية(الكوارث الطبيعية، والبرمجيات الخبيثة) في النتائج المباشرة للتهديدات بقوه تفسيرية متوسطة بلغت (24.1%) وفق الجداول رقم (24) و(25) و(26)، أما عن التهديدات الخارجية (المحترفين والقراصنة) فلم يتم التوصل إلى وجود أثر ذي دلالة إحصائية له في النتائج المباشرة ، وعلى هذا ، فانه يمكن القول إن (الكوارث الطبيعية ، والبرمجيات الخبيثة) تشكل تهديد حقيقياً للعمل الإلكتروني في جميع مراحله بدليل ظهور تأثير مرتفع لهذه التهديدات الأمنية على الرغم من عدم اكتمال مراحل الحكومة الإلكترونية في الوزارات المبحوثة ، أما عن تبرير عدم ظهور تأثير (للقراصنة والمحترفين) فهو نتيجة طبيعية مقترنة بالمرحلة الحالية التي وصل عندها التحول نحو الحكومة الإلكترونية والاتصال مايزال أحادي الجانب ،والمشاركة الخارجية غير مفعلة بعد لكن لايعني هذا الإغفال والتهاون بحجم الخطر الذي يشكله ذلك التهديد بل يجب التيقظ والحرص منه والتهيؤ لمواجهة تهديدهم الذي سوف ينشط فور بدء التشغيل الفعلي .

18- توصلت الدراسة إلى وجود أثر ذي دلالة إحصائية للتهديدات الخارجية(الكوارث الطبيعية ، والبرمجيات الخبيثة) في النتائج غير المباشرة للتهديدات بقوه تفسيرية متوسطة بلغت (26.8%) وفق الجداول رقم (27) و(28) و(29)، أما عن التهديدات الخارجية (المحترفين والقراصنة) فلم يتم التوصل إلى وجود أثر ذي دلالة إحصائية له في النتائج غير المباشرة ، وتتفق هذه النتائج جزئياً مع نتائج دراسة (الشواف والزالزله ،1999) ودراسة (Layen & Lee,2000) إذ

أكدت هذه الدراسات على أهمية توافر السرية والخصوصية والتكاملية لنجاح الحكومة الإلكترونية ، كما أظهرت تنوع مصادر التهديد للتكاملية .

19- توصلت الدراسة الى وجود فروق ذات دلالة إحصائية لاتجاهات المبحوثين نحو أثر التهديدات الأمنية في أمن المعلومات تعود لمتغيرات مثل (الجنس ، والعمر ،والمؤهل العلمي ، والمسمى الوظيفي) بينما لم تظهر هذه الفروقات لدى متغير (الخبرة) وذلك وفق الجدول رقم (30) .

التوصيات .

اعتماداً على الاستنتاجات المقدمة ، واستكمالاً لمستلزمات الدراسة ، ولغرض الإفادة منها ، فإنها تقدم عدداً من التوصيات هي :-

1- ضرورة التنبه إلى خطورة التهديدات الداخلية على أمن المعلومات ، لأن حجم الخسارة التي تخلفها كبيراً ، وبخاصه في حالة التهديد البشري لأنه يهدد الماديات والبرمجيات ، ويهز الثقة المتبادلة بين المنظمة والعاملين من جهة ، وبين المنظمة وجمهورها من جهة أخرى .

2- نظراً لأن بناء وإنشاء بنية تحتية وطنية شاملة ومتينة يشكل داعماً أساسي لتوفير الأمان لجميع العمليات الخدماتية والتجارية الإلكترونية ، فلا بد من الاهتمام بتجهيز الشبكات والأنظمة المساندة لها لتفادي حدوث أعطال تهز أمن الشبكات واستقرارها.

3-الحرص على الاحتفاظ بنسخ احتياطية من البرمجيات في مكان خارجي أثمن بشكل مستمر ودوري لتفادي نتائج التعرض لتهديد .

4- ضرورة وجود خطة طوارئ لكل منظمة بوصفها إجراءً وقائياً من الكوارث الطبيعية والتهديدات الأخرى ، والحرص على استخدام وسائل الحماية الفنية وغير الفنية ضد البرمجيات الخبيثة.

5- ضرورة توفير سياسة أمنية تحافظ على الموثوقية والخصوصية والتكاملية لكل منظمة تسعى إلى المحافظة على النظام المعلوماتي بأكمله لدعم نجاح الحكومة الإلكترونية.

6-ضرورة استحداث قسم خاص يعنى بالأمنية، وتعيين ضابط أمن معلومات في كل قسم يكون متعدد الاهتمامات (التنظيمية،والفنية، والقانونية) لأجل ضبط سير العمـل ومراقبـة تحركات العاملين في المنظمة.

7-ضرورة نشر الوعي والتثقيف للعاملين والمواطنين حول الحكومة الإلكترونية وخطورة التهديدات التي تعترض العمل الإلكتروني ، وذلك من خلال عقد دورات مستمرة للعاملين ، وقيام الوزارات المبحوثة بتخصيص مبالغ مالية ترصد لصالح دعم الإعلام حتى تكون التوعية شاملة تساهم في محو الأمية المعلوماتية في المجتمع.

8- ضرورة الاستفادة من تجارب الدول السابقة لنا في تطبيق الحكومة الإلكترونية مـع ضرورة مراعاة الفروق في الظروف والإمكانيات وتلافي الأخطاء التي حصلت في هـذه التجارب .

9- الحذر الشديد أثناء تطبيق الحكومة الإلكترونية من جانب الـوزارات المبحـوث لأن نجاح أو فشل تجربتها سوف ينعكس على بقية الوزارات عندما يتم تعميم التجربة ، ففـي حالة الفشل ستكون الخسائر كبيرة ومتعددة لذلك لابد من الحرص الشديد على نجاح هـذه التجربة .

10- ضرورة عمل دراسة متواصلة بشكل سريع تواكب السرعة الحاصـلة فـي عجلـة المعلوماتية والإلكترونية حول أبرز التهديدات الواقعة على العمل الإلكتروني وضـرورة تطوير وسائل أمن وحماية لكل تهديد جديد يتم اكتشافه حتى نسد الثغـرات الأمنيـة فـي أنظمة المعلومات الإلكترونية.

11-ضرورة الاهتمام بالجانب القانوني ، واستحداث وتطوير قوانين وأنظمه ومواد خاصة بالعمل الإلكتروني ، والجرائم المعلوماتية ذات الطابع الغامض والخطير الذي ينعدم فيـه ترك أثر لهذه الجرائم مع ضرورة التيقظ للسرعة المذهلة على صعيد المعلوماتيـة التـي تحتم على القانون السير بخطى سريعة أيضاً كما يجب إصدار قوانين رادعة للمعتـدين ، ومحاولة السعي لتحقيق تعاون محلي ودولي لمكافحة الجرائم المعلوماتية.

12- عدم تهاون من الإدارة العليا في مواصفات شاغلي الوظـائف فـي قسـم أنظمـة المعلومات الإلكترونية من (خبرة وتأهيل علمي وأخلاقيات وظيفية رفيعة) نظراً لحساسية هذه الوظائف وخطورتها.

قائمة المراجع

أ-المراجع العربية

ابن منظور ،أبو الفضل جمال الدين محمد بن مكرم ، (د . ت) ، لسان العـــــرب ، بيروت، دار صادر.

أبو علي ، عامر نزار ، (1994) ، فيروسات الكمبيـــــوتر ، ط1 ، عمان ، دار حنين .

أبو عياش، عبدالله، (1997)، "أمن البيانات بين الواقع والخيال"، مجلة الحاســوب، العدد 30، ص ص 16-17.

أبو موسى، أحمد، (2002) ،"جرائم الكمبيوتر:هل يمكنك حماية نظام المعلومــات المحاسبية الخاصة بك؟"، بحوث مؤتمر الإقتصاد والعلوم الإدارية، جامعة الزيتونة الأردنية، عمان، ص ص 609-625.

أحمد ، مروه ، (2002)،"الحكومة الإلكترونية من وجهه نظر موظفي القطاع الحكومي في الأردن" ، المؤتمر العلمي السنوي الثالث لكلية العلوم الإدارية والمالية المعرفة المعلوماتية والإدارة الإلكترونية، جامعة فيلادلفيا، عمان، ص ص 1-19.

بانكس، مايكل، (2001)، امن الكمبيوتر، ط1، ترجمة مركز التعريب والترجمة، بيروت ، الدار العربية للعلوم والنشر.

البداينة ، ذياب ، (2002)، الأمن وحرب المعلومات ، دار الشروق ، عمان.

بركات ،حسين وإبراهيم ،يحيى،(1990)، فيروسات الحاسب الآلي مرض عصر المعلومات،ط1، جدة، مطبوعات تهامة.

البشري، محمد الأمين،(1421)،"التحقيق في جرائم الحاسب الآلي والإنترنت" المجلة العربية للدراسات الأمنية والتدريب ، مجلد 15، العدد30، ص ص 317- 380 .

البياتي، هلال عبود، (1996)، "الوسائل الفنية لحماية البرامج ودور التشريع في حماية المعلومات"، مجلة أبحاث الحاسوب، مجلد1، العدد صفر، ص ص37-46.

جبر، محمد صدام، (2002)، "الموجة الإلكترونية القادمة:الحكومة الإلكترونية"مجلة الإداري، السنة 24، العدد 92، ص ص 167-209.

جريدة الدستور الأردنية، 3 شباط 2003، العدد 12759، الصفحة 29.

الجريدة الرسمية ، (1972)، رقم 2315، قانون حماية أسرار ووثائق الدولة، رقم 50 لسنة 1971، العدد2349.

حجازي، عبد الفتاح بيومي، (2002)،النظام القانوني لحماية التجارة الإلكترونية، ط1 ، الإسكندرية، دار الفكر الجامعي.

حسين، فاروق، (1999)، فيروسات الحاسب الآلي والإنترنت، ط1، الجيزة ، هلا للنشر والتوزيع.

حمودة، محمود عباس، (د.ت)، أمن الوثائق ، القاهرة ، دار غريب لطباعة.

الخطيب،أكرم ، (2000) ، "انخفاض نسبة قرصنة البرامج بالأردن" ، مجلة الحاسوب ، العدد 46،ص ص 19.

خليفات ، نزيه احمد ، (2002)، "قسم جرائم الحاسوب"، مجلة الشرطة، العدد 280، ص ص 30-31.

داوود ، حسن طاهر، (2000)، الحاسب وأمن المعلومات، ط1، الرياض، معهد الإدارة العامة.

داوود، سرحان والمشهداني، محمود، (2001)، أمن الحاسوب والمعلومات، ط1، عمان، دار وائل للطباعة والنشر.

الدباس، علي، (2003)"جرائم الحاسوب:تزوير معطيات الحاسوب"،مجلة الشرطة، العدد 283، ص ص 50-51 .

دونك، دي و دو يفينورين،(1996)، "الخصوصية كسياسة: منظور تطبيق السياسات الخاصة لحماية البيانات على مستوى القاعدة في هولندا" المجلة الدولية للعلوم الإدارية، معهد التنمية الإدارية الإمارات، مجلد 1، عدد4 (الإصدارالعربي)، مجلد 62، عدد 4 (الإصدار الإنجليزي).

رستم، هشام محمد، (2000)"الجرائم المعلوماتية"، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، ص ص 1-129.

الزعبي ، خالد، (2000)، "الأعمال الالكترونية والتجارة الالكترونية"، مجلة الحاسوب ، العدد 46، ص ص 12-13.

الزعبي، خالد، (2000)، "الحكومة الإلكترونية"، مجلة الحاسوب، العدد46، ص ص 13-14 .

الزعبي، خالد، (2002)، "الحكومة الإلكترونية"، مجلة الحاسوب، العدد54،ص ص 32-35.

الزعبي، خالد، (2002)، " السرية في الحكومة الالكترونية، "مجلة الحاسوب، العدد 54، ص ص 41-43.

الزعبي، خالد، (2002)، "المعايير الحيوية في حماية أمن المعلومات"، مجلة الحاسوب، العدد 53، ص ص 3-6.

الزعبي، عبده إبراهيم، (2003) "مفهوم الحكومة الإلكترونية في الأردن إمكانية التطبيق"، رسالة ماجستير غير منشورة ، جامعة النيلين.

زكي، يسرى عبد الحميد، (2001)، "أمن الكمبيوتر ضرورة أم ترف " مجلة عالم الكمبيوتر والانترنت، السنة الثالثة، العدد 32، ص ص 56-58.

سالم، فادي ، (2000)، " إدارة الأمن المنظور الواسع لأمن المعلومات" مجلة انترنت العالم العربي، العدد 10، ص ص 55.

سالم، فادي، (2000)، "أخطرما يهدد أمن الشبكة: نقاط الضعف والممارسات الخاطئة"، مجلة انترنت العالم العربي، العدد 11-ص ص 56.

سالم فادي، (200)، "كيف تصبح هاكراً"، مجلة إنترنت العالم العربي، العدد12 ، ص ص 56-57 .

سويدان، زياد، (1997)، أمـن الكمبيوتر بالأرقام مجلـة الحاسوب، العـدد 30، ص 20-21.

الشايع، ناصر علي، (1990)، فيروسات الحاسب الآلي مرض عصر المعلومات ، ط1، جده، مطبوعات تهامة.

شتا، محمد، (1998)، فكرة الحماية الجنائية لبرامج الحاسب الآلي، ط1، الإسكندرية، دارالجامعية الجديدة لنشر.

صالح، نائل عبد الرحمن، (2000)، "واقع جرائم الحاسوب في التشريع الجزائي الأردني" مؤتمر الكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، ص ص 1-19.

الصمادي، حازم نعيم، (2003)، المسؤولية في العمليات المعرفية الإلكترونية، ط1، عمان، دار وائل للطباعة والنشر.

طلبه، محمد، (د.ت)، الحاسب ونظم المعلومات الإدارية ، القاهرة، مجموعة كتب دلتا لتكنولوجيا علوم الحاسب.

عباس، حسن والفضلي، صلاح، (2001)، "خصوصية تقنية المعلومات من منظور نظرية المنفعة"، المجلة العربية للعلوم الإدارية، جامعة الكويت، مجلد8، العدد3، ص ص 347-369.

عبد النبي، طه ياسين،(2003)"الاختراق في شبكة الإنترنت"،المركز القومي للمختبرات الإنشائية،العراق،. Arab computing .come /haking . html http://internet ، ص ص 1-6.

عرب، يونس ، (2001)، قانون الكمبيوتر ، ط1 ، منشورات اتحاد المصارف العربية ، موسوعة القانون وتقنية المعلومات.

عرب، يونس، (2002) ، دليل أمن المعلومات والخصوصية : الخصوصية وحماية البيانات في العصر الرقمي، ط1، منشورات اتحاد المصارف العربية، موسوعة القانون وتقنية المعلومات.

عرب ، يونس،(2002) ،جرائم الكمبيوتر والإنترنت،ط1،منشورات اتحاد المصارف العربية ، موسوعة القانون وتقنية المعلومات.

العزام ،أحمد حسن،(2001)،"الحكومة الإلكترونية إمكانيات التطبيق"،رسالة ماجستير غير منشورة،جامعة اليرموك.

العواملة، نائل، (2002)، "الحكومة الإلكترونية ومستقبل الإدارة العامة: دراسةاستطلاعية للقطاع العام في دولة قطر"،مجلة دراسات العلوم الإدارية، مجلد29،العدد1،ص ص 146-162.

عوجان، عرفات، (2000)،"الحكومة الإلكترونية شروط النجاح"، مجلة الحاسوب، العدد47، ص ص10-11.

الغريب، انتصار نوري، (1994)، أمن الكمبيوتر والقانون ، بيروت، دار راتب الجامعية.

الغريب، انتصار نوري، (1994)، فيروسات الكمبيوتر، بيروت، دار راتب الجامعية.

القطامين، أحمد عواد، محمد، (2002)، الحكومة الإلكترونية دراسة تمهيدية، مؤتمر جامعة الزيتونة الأردنية تكنولوجيا المعلومات ودورها في التنمية الاقتصادية، ص ص 1-12.

الكيالي، إهاب، (2000)"الجمعية الأردنية للحاسبات تنظم ندوة علمية متخصصة بعنوان الحكومة الإلكترونية " ،مجلة الحاسوب ، العدد46، ص ص 11.

كيت، فريد هـ،(1999)،الخصوصية في عصر المعلومات،ط1، ترجمة محمد محمود شهاب ،مركز الأهرام للترجمة والنشر.

لطفي، محمد حسام، (1994)، الحماية القانونية لبرامج الحاسب الإلكتروني، أبحاث مؤتمر الكويت الأول للقانون والحاسب الآلي، جامعة الكويت.

محمد ، سليمان مصطفى ، (1419) ، "جرائم الحاسب وأساليب مواجهتها"، مجلة الأمن والحياة ، العدد 199، ص ص 49-51.

مركز المعلومات الوطني ، (1998) ، السياسة العامــة لنظام أمن وحماية المعلومات.

المسند، صالح وعبد الرحمن، المهيني، (1421)، "جرائم الحاسب الآلي الخطــر الحقيقي في عصر المعلومات"، المجلة العربية للدراسات الأمنية والتدريب، مجلد15، العدد 29، ص ص 147-207.

المناعسة، أسامة والزعبي، جلال والهواوشة، فاضل، (2001)، جرائم الحاسب الآلي والإنترنت، ط1 ، عمان ، دار وائل للطباعة والنشر.

منصور، محمد حسين، (2003)، المسؤولية الإلكترونية، الإسكندرية، دار الجامعة للنشر.

ب- المراجع الأجنبية

Alter, Steven,(1999),information systems, Addison-Wesley Educational, Publishers Inc .

Beheruz, Sethna & Cynthia C., Barnes,(1999),"E-Mail Communications In Colleges and Universities : are they privath?", Journal of education for Business, Vol.74 , Issue 6, PP.1-8 .

Chen, Yu-che & Gant, Jon,(2001),"Transforming Local e-government Services: the use of application Service providers", Government Information Quarterly, 18, PP.343-355

Cleary, Timothy,(1998), Information Technology, First Published, in Great Britain .

Deitel, H.M. & Deitel, P.J. & Nieto, T.R., (2001), E-Business & E- Commerce How To Program, Prentice Hall, New Jersey

Detmar w ., Straub ,(1998), "Coping with Systems Risk : Security Planning Models For Management Decision Making (NI)", MIS Quarterly , Vol 22 , Issue4, PP.1-31 .

Donn B, parker, (1996), "Ethics of information security", information management moral & thical, vol.5, Issue1,PP.1-6.

Joseph C., Panettieri, (1995)," Security", Information Week, Issue555,PP. (1-6) .

KanKanhalli,Atreyi & Teo,Hock-Hai & Tan,Bernardc.y & wei,kwok-kee,(2003),"An integrative study of information systems security effectiveness", International Journal of Information Management ,23,PP.139-154

Kevin, Hayes, (1997), "Information Technology-What Security Directors need to know" , International Security Review, Issue101,PP.1-6 .

Lanvin, Bruno, (2002), The E- Government Hand Book For Developing Countries, Aproject of Info Dev and The Center For Democracy & Technology .

Laudon,C.Kenneth & Laudon, Jane P.,(2000) ,Management Information Systems, Prentice – Hall, Inc .

Laudon, C. Kenneth & Laudon, Jane P., (2002), Managing information systems In the Digital Firm, Prentice – Hall, Inc

Layne, Karen & Lee ,Jungwoo ,(2001) , "Developing Fully Functional E-government : A four stage model", Government Information Quarterly , 18, PP.122-136 .

Marjory, Blumenthal , (1999), "The Politics and policies of enhancing trustworthiness for information systems", Communication Law & Policy, Vol4, Issue4, PP.1-35 .

Pacific Council, on international policy the western partner of the councilon forecin relation (2002) Roadmap for E-government in the Developing World. The working group on E-government .

Salem, Joseph A,(2003),"public and private Sector interests in e-government : a look at the Doe's pubscience", Government Information Quarterly,20,PP.13-27.

Timothy R , Stacey & Ronald E,Helsley ,(1996), "Identifying Information Security Threats", information systems Security,Vol5,Issue3,PP.1-31 .

Turban, Efaim & Lee, Jae & King, David & Chang, H.Michael,(2000),Electronic Commerce: Amanaerial Perspective, Prentice Hall, New Jersey .

Turban,EFRAI & McLean, Ephraim & Wetherbe, James, (1999), Information Technology for Management, Johnwiley & sons . Inc, New Yourk

ملحق رقم (1)

مجتمع الدراسة وعينتها

ملحق رقم (1)

جدول يبين أعداد مجتمع الدراسة وعينتها *

الرقم	الوزارة	مجتمع الدراسة	عينة الدراسة **
1-	الاتصالات وتكنولوجيا المعلومات	20	16
2-	المالية	32	28
3-	التخطيط	13	11
4-	الصناعة والتجارة	23	18
5-	أمانة عمان الكبرى	60	52
	المجموع	148	125

*لم تشمل الدراسة على رئاسة الوزراء وهي الطرف السادس والأخير من عينة الدراسة المشمول بالشبكة الآمنة وذلك بسبب طبيعة عملها الخاص .

** عينة الدراسة بنسبة (84.4%) من مجتمع الدارسة .

ملحق رقم (2)
استبانة الدراسة

ملحق رقم (2)

بسم الله الرحمن الرحيم

أخي المستجيب ... أختي المستجيبة المحترمون

تحية طيبة وبعد ،،،

صممت هذه الاستبانة للتعرف على أثـر التهديـدات الأمنيـة علـى امـن المعلومات في ضوء تطبيق الحكومة الالكترونية في عدد من الـوزارات الأردنيـة وأمانة عمان الكبرى . أرجو الإجابة على فقرات الاستبانة بموضوعية ودقه، شاكره لكم تعاونكم مؤكده ان المعلومات ستستخدم لأغراض البحث العلمي فقط .

وتفضلوا بقبول فائق الاحترام ،،،

آمنه ماجد الربيحات

يرجى وضع إشارة (×) أمام رمز الإجابة التي تنطبق عليك .

1- الجنـــــس : ☐ ذكر ☐ أنثى

2- العمــــــر : ☐ 29 سنه فأقل ☐ 30 - 39 سنه ☐ 40 - 49 سنه ☐ 50 سنه فأكثر

3- الخبــــرة : ☐ 5 سنوات فأقل ☐ 6 - 10 سنوات ☐ 11 - 15 سنه ☐ 16 سنه فأكثر

4- المؤهل العلمــي : ☐ الثانوية العامة فما دون ☐ الدبلوم المتوسط ☐ البكالوريوس ☐ الدراسات العليا

5- المسمى الوظيفي: ☐ إداريون ☐ فنيون ☐ مبرمجين ☐ مدخلي بيانات

ملاحظة / تفادياً لحصول سوء في فهم المصطلحات التاليــة (الموثوقيــة ، الخصوصية ، التكاملية) سيتم تعريفها بشكل مختصر :-

1-الموثوقية : هي حماية المعلومات و خلوها مــن أي إفســاد أو تزييــف أو التعرض للكشف غير المرخص مــع ضـمان تـوفر مصـداقية وأصــالة للمعلومات.

2-الخصوصية : هي حماية المعلومات الشخصية والأسـرار مـن التعـرض للإفشاء والكشف غير المشروع .

3- التكامليــــة : هي حماية المعلومات من التعديل غير المـرخص مــع ضمان سلامة محتوى المعلومات وتوفر المعلومات في وقت الحاجة لها .

يرجى وضع إشارة (×) أمام رمز الإجابة التي تنطبق عليك .

الرقم	الفقرة	تنطبق دائماً	تنطبق غالباً	تنطبق أحياناً	تنطبق نادراً	لا تنطبق أبدًا
1-	إن نماذج التحكم"المذكرات"المتعلقة بالتشغيل الإلكتروني في منظمتي تعد كافية.					
2-	إن تحديث الأنظمة بعد اكتشاف ثغرات أمنية فيها يتم على الفور					
3-	تستخدم كلمات مرور افتراضية في ربط الأنظمة التي يتم اختيارها بالإنترنت في منظمتي.					
4-	يتم التخلص من المخلفات التقنية(الأقراص والأوراق)الخاصة بالعمل الإلكتروني في المنظمة بصورة مناسبة.					
5-	الوسائل التقنية المستخدمة في حماية أنظمة المعلومات بالمنظمة تعتبر متطورة					
6-	يسمح بتداول كلمات السر بين الموظفين عبر الهاتف في منظمتي					
7-	إن العاملين في مجال المعلوماتية بالمنظمة يمتلكون مؤهلات تقنية جيدة					
8-	إن العاملين في مجال المعلوماتية بالمنظمة يمتلكون خبرات جيدة.					
9-	يخضع العاملون في مجال الأعمال الإلكترونية بالمنظمة لبرامج تدريبية بصورة مستمرة					
10	يخضع العاملون في الأعمال الإلكترونية بالمنظمة لعملية استقطاب وانتقاء محكمة.					
11-	يتوافر في المنظمة نظم لضبط ومراقبة تحركات العاملين.					
12-	يتوافر في منظمتي رقابة على البريد الصادر والوارد الخاص بالعاملين					
13-	تستخدم المنظمة إجراءات محددة في السماح للوصول إلى المعدات الإلكترونية والبرمجيات.					
14-	تستخدم المنظمة في منظوماتها الإلكترونية وسائل حمايـــة مــن الكوارث الطبيعية					
15-	توجد وسائل بديلة لتقديم الخدمة الإلكترونية في حال التعــرض إلى كارثة طبيعية.					
16-	يتم الاحتفاظ بنسخ إضافية من البرامج الإلكترونية توضع فـــي أماكن آمنة.					

رقم	الفقرة	تنطبق دائماً	تنطبق غالباً	تنطبق أحياناً	تنطبق نادراً	لا تنطبق أبدًا
-17	توجد خطط طوارئ خاصة بالعمل الإلكتروني في المنظمة في حال حصول كارثة طبيعية.					
-18	العمل الإلكتروني في المنظمة ليس عرضة للكوارث الطبيعية بصورة مستمرة.					
-19	تعتبر وسائل الحماية المطبقة في المنظمة ضد السرقات مناسبة					
-20	تستخدم المنظمة نظاماً للتشفير أثناء نقل البيانات					
-21	يتم اعتماد إجراءات سيطرة لمنع المتطفلين أو كشفهم في حال دخولهم على الشبكات.					
-22	يتم تغيير كلمات السر والشيفرات بشكل دوري.					
-23	تتعامل المنظمة بحرص أكبر مع المستفيد (الخارجي) صاحب الخبرة التقنية.					
-24	تتم مراقبة تحركات عمال الصيانة الإلكترونية الخارجيين.					
-25	يتم التأكد من سلامة المعدات الإلكترونية والبرامج المشتراة قبل استخدامها.					
-26	تستخدم في المنظمة برمجيات مضادة للفيروسات					
-27	تعتمد المنظمة على إجراءات سيطرة للحيلولة دون الوصول إلى برمجياتها مثل (أجهزة إنذار، مفاتيح)					
-28	يدرب العاملون بشكل مستمر على كيفية التعامل مع البرمجيات الخبيثة					
-29	إجراءات الحماية للعمل الإلكتروني بالمنظمة تحول دون تهديد البرامج الخبيثة					
-30	تتم توعية العاملين باستمرار حول الأساليب المتبعة لمواجهة تهديد البرمجيات الخبيثة.					
-31	تكثر الأعطال والتوقفات في الحاسوب الرئيسي Mainframe للمنظمة					
-32	إن حداثة الأجهزة والمعدات الإلكترونية المستخدمة لا تمنع حدوث أعطال وتوقفات متكررة.					
-33	تتصف الأضرار التقنية التي تتعرض لها المكونات المادية الإلكترونية بأنها بالغة.					
-34	يعد موقع مبنى الحاسوب الرئيسي هو السبب في تعرضه للعديد من التهديدات					

رقم	الفقرة	تنطبق دائماً	تنطبق غالباً	تنطبق أحياناً	تنطبق نادراً	لا تنطبق أبدًا
35-	تعتبر إجراءات تأمين الأجهزة المادية من (حاســبات وطابعــات) غير ملائمة					
36-	تتعرض البرمجيات التطبيقية إلى تهديد خارجي أو / وداخلي من حين لآخر.					
37-	على الرغم من حزم الأمان المستخدمة لتأمين البرمجيات والتطبيقات، فإنها عرضه لتهديدات المستمرة.					
38-	اختلاف بيئة عمل المنظمة ليس له أثر على سلامة نظم التشغيل المستخدمة.					
39-	إن معظم التهديدات لقواعد بيانات المنظمة هو من أفراد غير متخصصين.					
40-	إن عدم تحديد الفئات المستخدمة لقواعد بيانات المنظمة يجعلها عرضة للتهديد.					
41-	تفتقد إدارة قواعد البيانات إلى خطة لتأمين البيانات					
42-	إن المشكلات في أنظمة تشغيل الشبكة أو الأنظمة المساندة تؤدي إلى تهديد أمن الشبكة المحلية.					
43-	أن نوع الشبكات المستخدمة يقود إلى حدوث أعطال ذات طبيعة تقنية.					
44-	تؤدي الأخطاء البشرية إلى حدوث أعطال في أجزاء الشبكة.					
45-	تفتقد الشبكات المحلية إلى وسائل مادية كافية لتأمينها.					
46-	تتوافر الموثوقية في العمل الإلكتروني للمنظمة.					
47-	لا تتعرض مصداقية المعلومات المتوافرة إلى الاعتداء.					
48-	تعتبر المعلومات الخاصة بالعمل غير متاحة بين جميع المخولين.					
49-	يشكو المتعاملون مع المنظمة بانتهاك مبدأ الخصوصية.					
50-	يعتبر كشف الأرقام السرية والتنصت من أبرز ما يهدد الخصوصية في المنظمة.					
51-	تفتقد المنظمة إلى سياسة واضحة ومحددة لحماية الخصوصية.					
52-	تعمل جميع البرامج بشكل يؤدي إلى سلامة المعلومات.					
53-	أن السياسة الأمنية التي تطبقها المنظمة تقود إلى تحقيق التكاملية.					
54-	لا يتعرض محتوى المعلومات إلى التعديل نتيجة التدخل غير المشروع في المنظمة.					

يرجى وضع إشارة (×) عند الإجابة التي تعبر عن رأيك في الفقرات التالية :

الرقم	الفقرة	نعم	لا
1-	هنالك قسم خاص مسؤول عن أمن المعلومات وحمايتها في المنظمة .		
2-	هنالك أسس لتصنيف أمنية المعلومات ودرجة سريتها .		
3-	هنالك معايير وأسس تستخدم باعتبارها ضوابط أمنية للأفراد .		
4-	هنالك رقابة مستمرة من الإدارة العليا على الإجراءات الأمنية .		
5-	يوجد في المنظمة وظيفة بمسمى ضابط أمن معلومات .		
6-	توجد إجراءات تقنية في المنظمة للمحافظة على المحطات الطرفية وسلامتها.		
7-	يتم عمل صيانة دورية لمراكز الحاسوب وتقنياته في المنظمة .		
8-	يتم عمل صيانة دورية لأنظمة ووسائل الأمان في المنظمة .		
9-	هنالك سجل يضبط تحركات عمال الصيانة الداخلين .		
10	يوجد قسم داخل المنظمة يهتم بالشؤون القانونية المتعلقة بالحاسوب .		
11-	توجد عقوبات بحق من يعتدي على أمنية المعلومات .		
12-	تتخذ المنظمة إجراءات صارمة بحق من يكشف أسرار العمل المتعلقة بالمهنة.		
13-	تتخذ المنظمة إجراءات صارمة بحق من يكشف أسرار العمل المتعلقة بالمراجعين ومعاملاتهم .		
14-	تنظم عملية أمن وحماية المعلومات بوساطة السلطة التشريعية .		

ملحق رقم (3)

أعضاء هيئة تحكيم أداة الدراسة

ملحق رقم (3)

أعضاء هيئة تحكيم الدراسة مرتبة أسماؤهم حسب الألقاب العلمية

الاســــــــــم	الرتبة الأكاديمية	التخصص
الدكتور محمد الطائـــــي	أستـــــاذ	نظم معلومات
الدكتور زياد المعشـــــر	أستاذ مشارك	إدارة عامة
الدكتور عبدالرزاق الشيخلي	أستاذ مشارك	إدارة عامة
الدكتورة ماجدة العطيـــة	أستاذ مشارك	إدارة أعمال
الدكتور أحمد القطاميـــن	أستاذ مشارك	إدارة أعمال
الدكتور نضال الحوامـــده	أستاذ مشارك	إدارة عامة
الدكتور موفق فتحـــــي	أستاذ مشارك	تكنولوجيا معلومات
الدكتور محمود العمـــري	أستاذ مشارك	حاسوب
الأستاذ بسام المحاديـــن	محاضر متفرغ	حاسوب
الأستاذ محمد الربابعـــه	محاضر متفرغ	حاسوب